VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

Ministero dell'Istruzione e del Merito

Dipartimento per le risorse umane, finanziarie e strumentali

Direzione generale per i sistemi informativi e la statistica

Ministero della Cultura

Direzione Generale Archivi

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

Manuale per la gestione dei flussi documentali

"Liceo Scientifico Da Vinci"

Firmato digitalmente da Frighetto Iole Antonella

PREMESSA **3**

GLOSSARIO **3**

ACRONIMI 3

1. 4

1.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO 4

1.2 FORME DI PUBBLICITÀ E DIVULGAZIONE 4

2. 5

2.1. AREA ORGANIZZATIVA OMOGENEA 5

2.2. RUOLI E RESPONSABILITÀ 5

2.3. MODELLO ORGANIZZATIVO ADOTTATO 8

2.4. CASELLE DI POSTA ELETTRONICA 8

3. 10

3.1. PROCESSO DI PRODUZIONE E GESTIONE 9

3.1.1. Processo di produzione e gestione - Acquisizione 10

3.1.2. Processo di produzione e gestione - Creazione 13

3.1.3. Processo di gestione - Classificazione 14

3.1.4. Processo di gestione - Fascicolazione 14

3.1.5. Processo di gestione - Archiviazione 16

3.2. PROCESSO DI CONSERVAZIONE 18

3.2.1. Versamento in archivio di deposito 19

3.2.2. Scarto 19

3.2.3. Versamento in archivio storico 20

3.2.4. Delocalizzazione 20

4. 22

4.1. DOCUMENTO RICEVUTO 21

4.2. DOCUMENTO INVIATO 22

4.3. DOCUMENTO DI RILEVANZA ESTERNA 22

4.4. DOCUMENTO DI RILEVANZA INTERNA 22

4.5. DOCUMENTO ANALOGICO 22

4.6. DOCUMENTO INFORMATICO 23

4.6.1. Le firme elettroniche 24

4.7. CONTENUTI MINIMI DEI DOCUMENTI 26

4.8. PROTOCOLLABILITÀ DI UN DOCUMENTO 27

5. 30

5.1. PROTOCOLLAZIONE 27

Firmato digitalmente da Frighetto Iole Antonella

5.2. SCRITTURA DI DATI DI PROTOCOLLO 28
5.3. SEGNATURA DI PROTOCOLLO 29
5.4. DIFFERIMENTO DELLA REGISTRAZIONE DI PROTOCOLLO 30
5.5. RICEVUTA DI AVVENUTA PROTOCOLLAZIONE 30
5.6. REGISTRO GIORNALIERO DI PROTOCOLLO 30
5.7. REGISTRO DI EMERGENZA 31
5.8. REGISTRI PARTICOLARI 32
5.9. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO 32
5.10. MODALITÀ DI SVOLGIMENTO DEL PROCESSO DI SCANSIONE 32

6. 42

6.1. TUTELA DEI DATI PERSONALI E MISURE DI SICUREZZA 33
6.2. DIRITTO DI ACCESSO AGLI ATTI 35
6.2.1. Accesso documentale 35
6.2.2. Accesso civico generalizzato (FOIA) 36
6.2.3. Registro degli accessi 38

Firmato digitalmente da Frighetto Iole Antonella

PREMESSA

Le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, prevedono l'obbligo per le Pubbliche Amministrazioni di redigere con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale.

Il presente Manuale di gestione documentale, adottato dall'Istituzione scolastica "Liceo Scientifico Da Vinci" al fine di adeguarsi alle disposizioni di cui sopra, descrive il sistema di gestione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel dettaglio, il Manuale descrive il modello organizzativo adottato dalla scuola per la gestione documentale e il processo di gestione del ciclo di vita del documento, oltre a fornire specifiche istruzioni in merito al documento amministrativo ed al documento informatico, al protocollo informatico e alle tematiche di accesso, trasparenza e *privacy*.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Pertanto, il presente documento si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con gli organi dell'Istituto.

GLOSSARIO

ACRONIMI

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e ss.mm.ii.)
D.L.	Decreto-legge
D.Lgs.	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
D.P.R.	Decreto del Presidente della Repubblica
DSGA	Direttore dei Servizi Generali e Amministrativi
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
iPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RPD	Responsabile della protezione dei dati
RPCT	Responsabile per la prevenzione della corruzione e della trasparenza
RUP	Responsabile unico del procedimento
UOR	Unità Organizzativa Responsabile

Firmato digitalmente da Frighetto Iole Antonella

1. IL MANUALE DI GESTIONE DOCUMENTALE

Il presente manuale descrive il sistema di produzione e gestione dei documenti, anche ai fini della conservazione.

In coerenza con il quadro normativo di riferimento, il manuale è volto a disciplinare le attività di creazione, acquisizione, registrazione, classificazione, assegnazione, fascicolazione e archiviazione dei documenti informatici, oltre che la gestione dei flussi documentali e archivistici dell'Istituzione scolastica, nonché, seppur in via residuale, la gestione dei documenti non informatici. Tali attività sono finalizzate alla corretta identificazione e reperibilità dei documenti acquisiti e creati dalla scuola nell'ambito dell'esercizio delle proprie funzioni amministrative.

Il manuale, dunque, costituisce una guida dal punto di vista operativo per tutti coloro che gestiscono documenti all'interno dell'Istituzione scolastica, in modo tale da facilitare un corretto svolgimento delle operazioni di gestione documentale.

1.1 MODALITÀ DI APPROVAZIONE E AGGIORNAMENTO

Il Responsabile della gestione documentale[1] si occupa della predisposizione del manuale, che è adottato con provvedimento dal Dirigente Scolastico.

Il manuale deve essere aggiornato periodicamente effettuando il censimento delle attività/prassi in essere, la razionalizzazione delle stesse, l'individuazione e la definizione degli aspetti organizzativi e gestionali in termini di fasi, tempi e risorse umane impegnate nell'automazione dei flussi documentali nel rispetto della normativa.

Ogni evento suscettibile di incidere sull'operatività ed efficacia del manuale medesimo deve essere tempestivamente segnalato al Responsabile della gestione documentale, al fine di prendere gli opportuni provvedimenti in ordine all'eventuale modifica e/o integrazione della procedura stessa.

1.2 FORME DI PUBBLICITÀ E DIVULGAZIONE

In coerenza con quanto previsto nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*"[2] (a seguire, anche "Linee Guida"), adottate dall'AgID con Determinazione n. 407/2020 ed in seguito aggiornate con Determinazione n. 371/2021 (da attuare entro il 1° gennaio 2022), ovvero che il manuale sia reso pubblico mediante la pubblicazione sul sito istituzionale in una parte chiaramente identificabile dell'area "Amministrazione trasparente", prevista dall'art. 9 del D.Lgs. 33/2013,[3] il presente manuale è

[1] Per ulteriori dettagli in merito a tale figura, si veda il par. "2.2. - Ruoli e responsabilità".

[2] Si ricorda che le Linee Guida AgID hanno carattere vincolante, come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al D.Lgs. 82/2005 n. 2122/2017 del 10.10.2017. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2, del citato D.Lgs. 82/2005, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del medesimo Codice.

[3] L'art. 9, comma 1, del D.lgs. 33/2013, prevede che: "*Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Al fine di evitare eventuali duplicazioni, la suddetta pubblicazione può essere sostituita da un collegamento ipertestuale alla*

Firmato digitalmente da Frighetto Iole Antonella

reso disponibile alla consultazione del pubblico mediante la diffusione sul sito istituzionale dell'Istituzione scolastica.

2. IL MODELLO ORGANIZZATIVO

2.1. AREA ORGANIZZATIVA OMOGENEA

L'art. 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 "*Testo unico delle disposizioni legislative e regolamentari in materia di regolamentazione amministrativa*" stabilisce che "*Ciascuna Amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse*".

L'Istituzione scolastica individua al proprio interno un'unica Area Organizzativa Omogenea (AOO), alla quale corrisponde un Registro unico di protocollo, denominato REGISTRO PROTOCOLLO.

L'AOO può essere sotto-articolata in Unità Organizzative Responsabili (UOR), ovvero l'insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

L'articolazione delle AOO e delle eventuali UOR sono riportate in allegato (7.1).

L'allegato di cui sopra è suscettibile di modifiche. L'inserimento/cancellazione/aggiornamento delle UOR deve essere formalizzato con provvedimento a firma del Responsabile della gestione documentale e recepito nel presente manuale.

2.2. RUOLI E RESPONSABILITÀ

L'Istituzione scolastica, allo scopo di assicurare un trattamento uniforme dei documenti, una puntuale applicazione delle disposizioni ed un periodico monitoraggio delle modalità d'uso degli strumenti di gestione documentale, deve prevedere al suo interno le seguenti figure:

- il **Responsabile della gestione documentale** ed il suo vicario[4];
- il **Responsabile della conservazione**;
- il **Responsabile per la prevenzione della corruzione e della trasparenza**;
- il **Responsabile della protezione dei dati**, ai sensi dell'art. 37 del Regolamento UE 679/2016.

Inoltre, in aggiunta alle figure sopra elencate, si evidenzia la rilevanza di individuare il **Referente per l'indice delle Pubbliche Amministrazioni** (iPA), soggetto a cui il Dirigente Scolastico affida il compito, sia organizzativo che operativo, di interagire con il gestore dell'iPA

---

sezione del sito in cui sono presenti i relativi dati, informazioni o documenti, assicurando la qualità delle informazioni di cui all'articolo 6. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

[4] Come definito nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID "*Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a: […] nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche*".

Firmato digitalmente da Frighetto Iole Antonella

per l'inserimento e la modifica dei dati dell'Istituzione scolastica, nonché per ogni altra questione riguardante la presenza della stessa presso l'iPA[5].

Il **Responsabile della gestione documentale** è il soggetto in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.

Tenuto conto di quanto sopra, il Responsabile della gestione documentale è individuato, all'interno dell'Istituzione scolastica, nella persona del Dirigente Scolastico Frighetto Dott.ssa Iole Antonella[6].

Il Responsabile della gestione documentale ed il suo vicario sono nominati con apposito provvedimento del Dirigente Scolastico.

Il **Responsabile della conservazione** è il soggetto in possesso di idonee competenze giuridiche, informatiche ed archivistiche, che opera secondo quanto previsto dall'art. 44, comma 1-*quater*, del D.Lgs. 82/2005 (di seguito anche "CAD")[7].

In particolare, il Responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli *standard* internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

---

[5] Le *"Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (IPA)", adottate dall'AgID, al paragrafo 2.2, stabiliscono che "*Il Responsabile dell'Ente nell'istanza di accreditamento nomina un Referente IPA che ha il compito di interagire con il Gestore IPA per l'inserimento e la modifica dei dati, nonché per ogni altra questione riguardante la presenza dell'Ente nell'IPA*".

[6] Si precisa che, anche nell'ipotesi in cui il Responsabile della gestione documentale venga individuato in una figura diversa dal Dirigente Scolastico, alcuni compiti e responsabilità restano in capo allo stesso Dirigente, nel rispetto delle previsioni contenute nell'art. 4, comma 2, e nell'art. 25 del D.Lgs. 165/2001.

[7] L'art. 44, comma 1-*quater*, del CAD prevede che: "*Il responsabile della conservazione, che opera d'intesa con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis*".

Firmato digitalmente da Frighetto Iole Antonella

f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità, adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[8];
m) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in *outsourcing* dalle Pubbliche Amministrazioni.

Il ruolo del Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale o anche da altre figure. Tenuto conto di quanto sopra, il Responsabile della conservazione è individuato, all'interno dell'Istituzione scolastica, nella persona del Dirigente Scolastico.

Il Responsabile della conservazione è nominato con apposito decreto del Dirigente Scolastico.

Il **Responsabile per la prevenzione della corruzione e della trasparenza** (RPCT) è il soggetto al quale può essere presentata l'istanza di accesso civico, qualora la stessa abbia ad

[8] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "*Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio*".

Firmato digitalmente da Frighetto Iole Antonella

oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013[9].

Il RPCT, oltre a segnalare i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, si occupa delle richieste di riesame dei richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso civico generalizzato, ovvero che non abbiano avuto alcuna risposta entro il termine stabilito (si veda, per maggiori dettagli quanto specificato nel paragrafo 6.2.2).

Il **Responsabile della protezione dei dati** (RPD) è il soggetto nominato con apposito decreto del Dirigente Scolastico, che ha il compito di sorvegliare sull'osservanza della normativa in materia di protezione dei dati personali, ossia il Regolamento UE 679/2016 (di seguito, anche "GDPR") e il D.Lgs. 196/2003 (di seguito, anche "Codice *privacy*") come modificato dal D.Lgs. 101/2018.

Il Responsabile della protezione dei dati deve essere coinvolto in tutte le questioni che riguardano la gestione e la protezione dei dati personali e ha il compito sia di informare e sensibilizzare il personale della scuola riguardo agli obblighi derivanti dalla citata normativa sia di collaborare con il Titolare e il Responsabile del trattamento, laddove necessario, nello svolgimento della valutazione di impatto sulla protezione dei dati[10].

Sul punto, le "*Linee Guida sui responsabili della protezione dei dati*", adottate dal WP29 il 13 dicembre 2016, emendate in data 5 aprile 2017, precisano che "*Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento*".

Per ciò che concerne le modalità attraverso le quali il Responsabile della protezione dei dati si interfaccia con il Responsabile della gestione documentale e con il Responsabile della conservazione in merito all'adozione delle misure di sicurezza del sistema di gestione informatica dei documenti, si rimanda a quanto descritto nel dettaglio al paragrafo 6.1.

---

[9] Art. 5, comma 3, lett. d), D.Lgs. 33/2013.

[10] La figura del Responsabile della protezione dei dati è disciplinata dal Considerando n. 97 e dagli artt. 37 – 39 del Regolamento UE 679/2016, nonché dalle Linee guida sui responsabili della protezione dei dati, già richiamate nel testo (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287*). Tale figura ha il compito di: valutare i rischi di ogni trattamento; collaborare con il Titolare/Responsabile del trattamento, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati; informare e sensibilizzare il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati; cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; supportare il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento. Il Responsabile della protezione dei dati è individuato tra i soggetti in possesso di specifici requisiti, competenze professionali e conoscenze specialistiche in materia di protezione dei dati, in linea con le funzioni che è chiamato a svolgere e che deve poter adempiere in piena indipendenza e in assenza di conflitti di interesse.

Firmato digitalmente da Frighetto Iole Antonella

2.3. MODELLO ORGANIZZATIVO ADOTTATO

[Nel caso di adozione di un sistema accentrato]

Il sistema di protocollazione è unico per l'Istituzione scolastica e viene adottato un sistema "accentrato", per cui tutte le comunicazioni sono gestite, sia in ingresso che in uscita, da un'unica UOR che si occupa della loro protocollazione. In dettaglio:

- le **comunicazioni in ingresso**, indipendentemente dalla tipologia di comunicazione (via PEC, PEO o formato cartaceo) giungono presso il punto unico di accesso, dove vengono registrate a protocollo e smistate nelle diverse UOR a seconda della competenza;
- le **comunicazioni in uscita** sono trasmesse ad un'unica UOR, che si occupa della loro protocollazione e del loro invio.

[Nel caso di adozione di un sistema parzialmente accentrato]

Il sistema di protocollazione adottato dall'Istituzione scolastica è "parzialmente accentrato", per cui tutte le comunicazioni giungono al punto unico di accesso mentre possono essere trasmesse in uscita da tutte le UOR. In dettaglio:

- le **comunicazioni in ingresso**, indipendentemente dalla tipologia di comunicazione (via PEC, PEO o formato cartaceo) giungono presso il punto unico di accesso, dove vengono registrate a protocollo e smistate nelle diverse UOR a seconda della competenza;
- le **comunicazioni in uscita** sono trasmesse in uscita dalle singole UOR.

Le UOR e i soggetti abilitati per la ricezione, l'assegnazione, la consultazione, la protocollazione, la classificazione e l'archiviazione dei documenti sono individuati dal Responsabile della gestione documentale mediante atti organizzativi interni.

2.4. CASELLE DI POSTA ELETTRONICA

L'Istituzione scolastica è dotata di una casella di Posta Elettronica Certificata (PEC) istituzionale per la gestione del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. L'indirizzo PEC deve essere pubblicato sull'indice delle Pubbliche Amministrazioni.

La casella di cui sopra costituisce l'indirizzo virtuale della sede legale dell'AOO. Inoltre, l'Istituzione scolastica si avvale delle seguenti caselle PEC "di servizio" opportunamente autorizzate ed attivate, per le quali si descrivono i termini e le modalità d'uso: vips08000d@pec.istruzione.it e vips08000d@istruzione.it.

L'Istituzione scolastica è dotata anche di una casella di Posta Elettronica Ordinaria (PEO) istituzionale, utile a gestire i messaggi di posta elettronica con annessi documenti ed eventuali allegati, aventi rilevanza amministrativa.

Firmato digitalmente da Frighetto Iole Antonella

Inoltre, l'Istituzione scolastica si avvale di caselle di Posta Elettronica Ordinaria interne ("di servizio") da affidare alla gestione di una UOR o del singolo operatore[11].

Le disposizioni vincolanti inerenti ai termini e modalità d'uso delle PEC e delle PEO sono pubblicati sul sito istituzionale dell'Istituzione scolastica.

3. IL CICLO DI VITA DEL DOCUMENTO

Il ciclo di vita del documento è articolato nei processi di produzione, gestione e conservazione:

- il **processo di produzione** del documento si sostanzia principalmente nell'acquisizione di documenti cartacei, informatici e/o telematici ovvero nella creazione degli stessi;
- il **processo di gestione** interessa tutte le attività a partire dalla registrazione del documento, alla classificazione, assegnazione e fascicolazione/archiviazione corrente;
- il **processo di conservazione** si sostanzia nel trasferimento dei documenti dall'archivio corrente all'archivio di deposito (dal quale possono eventualmente seguire l'attività di scarto e di delocalizzazione) e dall'archivio di deposito all'archivio storico.

Nei paragrafi successivi si riporta una panoramica dei processi suddivisi per:

- processo di produzione e gestione;
- processo di conservazione.

3.1. PROCESSO DI PRODUZIONE E GESTIONE

Il processo di produzione e gestione fornisce una sintesi delle attività da porre in essere con riferimento sia alla produzione del documento, sia alle fasi di gestione dello stesso. Il processo di produzione è suddiviso in "Processo di produzione - Acquisizione" e "Processo di produzione - Creazione", al fine di distinguere rispettivamente le attività relative ai documenti in entrata dalle attività relative ai documenti elaborati dall'Istituzione scolastica.

Con riferimento alla gestione del documento, si fornisce un dettaglio delle seguenti fasi: classificazione, fascicolazione, archiviazione.

3.1.1. PROCESSO DI PRODUZIONE E GESTIONE - ACQUISIZIONE

Il "Processo di produzione e gestione – Acquisizione" è descritto differenziando il caso in cui l'*input* sia un documento cartaceo dal caso in cui sia informatico, dato che i documenti provenienti dall'esterno possono essere di natura cartacea o di natura informatica.

[11] Ai sensi della Direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie, "*Appare, perciò, necessario che le pubbliche amministrazioni provvedano a dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e ad attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza.*"

Firmato digitalmente da Frighetto Iole Antonella

Nel caso di **documento cartaceo in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente:

- rilascia una ricevuta timbrata, qualora il documento dovesse essere consegnato a mano[12];
- verifica la competenza del documento stesso.

Nel caso di documenti pervenuti erroneamente all'Istituzione scolastica ma indirizzati ad altri soggetti, il documento:

- si restituisce per posta;

oppure

- se la busta che lo contiene viene aperta per errore, è protocollato in entrata e in uscita, inserendo nel campo oggetto e nel campo di classificazione la nota "Documento pervenuto per errore", ed è rinviato al mittente apponendo sulla busta la dicitura "Pervenuta ed aperta per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto alla protocollazione:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla scansione e alla successiva verifica di conformità all'originale della copia informatica (cfr. par. "5.10. - Modalità di svolgimento del processo di scansione");
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza previste al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione;
- provvede alla protocollazione in ingresso del documento;
- appone il timbro contenente i dati contenuti nella segnatura di protocollo tramite l'apposita funzionalità del servizio di protocollo informatico ovvero, solo in caso di impossibilità, procede manualmente.

Nella fase di assegnazione, l'operatore addetto alla protocollazione provvede all'assegnazione del documento al personale competente secondo le seguenti modalità e regole di assegnazione [*modalità e regole di assegnazione*]. Il Responsabile della gestione documentale, ovvero il vicario, può, in ogni caso, rettificare l'assegnatario del documento.

Successivamente alle fasi di registrazione, classificazione e assegnazione, è necessario procedere con la fase di fascicolazione/archiviazione del documento.

[12] Il servizio protocollo non rilascia, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. La semplice apposizione del timbro datario sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale amministrativo della scuola in merito alla ricezione ed all'assegnazione del documento.

Firmato digitalmente da Frighetto Iole Antonella

[Nel caso di conservazione ibrida]

Per i documenti cartacei, si provvede alla conservazione ibrida, in cui è prevista la conservazione sia del documento analogico originale sia della copia informatica. Pertanto, il Responsabile della gestione:

- inserisce il documento cartaceo in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

[Nel caso di conservazione sostitutiva]

Per i documenti cartacei, si provvede alla conservazione sostitutiva, con la quale è garantita nel tempo la validità legale di un documento informatico, inteso come una rappresentazione di atti o fatti e dati su un supporto sia esso analogico o informatico. Pertanto, il Responsabile della gestione:

- attesta la conformità del documento informatico al documento cartaceo, ai sensi dell'art. 22, comma 2, del CAD;
- può distruggere il documento cartaceo;
- inserisce il documento informatico in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

Si precisa che non possono essere distrutti i documenti elencati dal DPCM 21 marzo 2013[13], per i quali rimane l'obbligo della conservazione del cartaceo anche nel caso di conservazione sostitutiva.

[In entrambi i casi (conservazione ibrida e conservazione sostitutiva)]

Per tali attività, il Responsabile della gestione può disporre apposita delega all'assegnatario o ad altro personale appositamente individuato.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

---

[13] L'Allegato al DPCM 21 marzo 2013 avente ad oggetto "*Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*", riporta tra i documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo, i seguenti:
a) atti contenuti nella Raccolta ufficiale degli atti normativi della Repubblica;
b) atti giudiziari, processuali e di polizia giudiziaria per i venti anni successivi;
c) opere d'arte;
d) documenti di valore storico – artistico, ivi compresi quelli in possesso delle forze armate;
e) documenti, ivi compresi quelli storico – demaniali, conservati negli archivi, nelle biblioteche e nelle discoteche di Stato, ivi compresi gli atti e documenti conservati nella biblioteca storica dell'ex Centro Studi Esperienze della Direzione Centrale per la prevenzione e la Sicurezza Tecnica del Dipartimento dei V.V.F., de soccorso pubblico e della difesa civile;
f) atti notarili;
g) atti conservati dai notai ai sensi della legge 16 febbraio 1913, n. 89, prima della loro consegna agli Archivi notarili;
h) atti conservati presso gli Archivi notarili.

Firmato digitalmente da Frighetto Iole Antonella

Nel caso di **documento informatico in ingresso**, nella fase di acquisizione, l'Istituzione scolastica ricevente verifica la competenza del documento.

Nel caso di documenti pervenuti erroneamente sulla casella PEC o PEO dell'Istituzione scolastica, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore – non di competenza di questa Amministrazione". Inoltre, se il documento è stato erroneamente protocollato, l'addetto al protocollo provvede ad annullare la registrazione, secondo le modalità descritte nel presente manuale, oppure a protocollare il documento in uscita indicando come oggetto "Protocollato per errore".

Se il documento è di competenza dell'Istituzione scolastica ricevente, segue la fase di registrazione in cui l'operatore addetto al protocollo:

- valuta se il documento è da protocollare (cfr. par. "4.8. - Protocollabilità di un documento");
- nel caso in cui il documento sia da protocollare procede alla verifica di validità della firma (se presente)[14];
- verifica la presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016, ai fini dell'attuazione delle misure di sicurezza di cui al paragrafo 6.1;
- provvede alla classificazione del documento sulla base del titolario di classificazione[15];
- provvede alla protocollazione in ingresso.

Nella fase di assegnazione l'operatore addetto al protocollo provvede ad assegnare il documento al personale competente. Il Responsabile della gestione documentale può, in ogni caso, rettificare l'assegnatario del documento.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici, le Istituzioni scolastiche, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

Con la conservazione digitale si esegue la fase di fascicolazione/archiviazione corrente in cui gli utenti opportunamente abilitati provvedono all'inserimento del documento informatico o in un nuovo fascicolo o in un fascicolo già esistente all'interno dell'archivio corrente elettronico.

[14] Per ulteriori approfondimenti, si veda il cap. "4. - Il documento amministrativo".

[15] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

Firmato digitalmente da Frighetto Iole Antonella

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.

3.1.2. Processo di produzione e gestione - Creazione

Nel "Processo di produzione e gestione – Creazione", si considera come *input* del processo esclusivamente il documento di natura informatica (cfr. par. "4.6. - Documento informatico").

Nella fase di creazione, il documento:

- è elaborato dal personale competente ed inviato al Dirigente o altro personale responsabile (ad es. DSGA) per la revisione dello stesso, ovvero è elaborato dal Dirigente stesso;
- è successivamente approvato o dal Dirigente o da altro personale responsabile in base alla competenza.

Nella fase di elaborazione e revisione, è possibile fare circolare il documento tra i soggetti interessati registrandolo come "bozza".

I documenti informatici prodotti, indipendentemente dal *software* utilizzato per la loro creazione, prima della loro sottoscrizione con firma digitale, sono convertiti in uno dei formati *standard* previsti dalla normativa vigente[16], al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "*Formati di file e riversamento*" delle Linee Guida, effettuando una valutazione di interoperabilità, svolta in base alle indicazioni previste nel medesimo Allegato[17].

I formati utilizzati dall'Istituzione scolastica, secondo la valutazione di interoperabilità, sono: PDF, XML e TIFF.

Nella fase di registrazione l'operatore di protocollo provvede:

- alla verifica della presenza di categorie particolari di dati personali, di cui all'articolo 9 del Regolamento UE 679/2016;
- alla classificazione del documento sulla base del titolario di classificazione[18];

[16] Allegato 2 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

[17] La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati. Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.

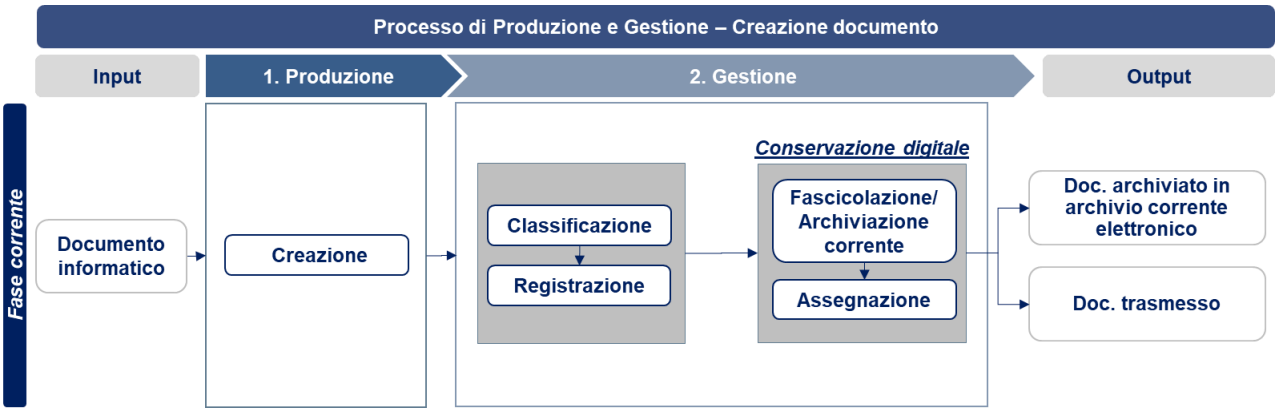
Firmato digitalmente da Frighetto Iole Antonella

- alla registrazione di protocollo.

Nella fase di fascicolazione/archiviazione corrente l'operatore di protocollo provvede all'inserimento del documento informatico in un fascicolo già esistente o, nel caso in cui il fascicolo non sia presente, provvede a crearlo oppure a richiederne la creazione all'utente opportunamente abilitato.

Successivamente alla fase di fascicolazione/archiviazione, il documento può essere oggetto di una nuova assegnazione o di pubblicazione.

Di seguito si fornisce la rappresentazione grafica del processo sopra descritto.



3.1.3. Processo di gestione - Classificazione

La classificazione è l'operazione obbligatoria che consente di organizzare i documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Istituzione scolastica. Essa è eseguita a partire dal titolario di classificazione.

Il titolario unico di classificazione, in allegato (7.2), è l'insieme delle voci logiche gerarchicamente strutturate e articolate in gradi divisionali (titolo/classe/eventuale sottoclasse), stabilite sulla base delle funzioni dell'Amministrazione. Esso è definito con apposito decreto del Dirigente Scolastico ed è unico a livello di Istituzione scolastica.

Tutti i documenti ricevuti e prodotti dall'Istituzione scolastica, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario di classificazione; mediante tale operazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe e eventuale sottoclasse), anche il numero di repertorio del fascicolo. L'operazione suddetta è obbligatoria all'atto della registrazione di protocollo, ma è possibile effettuare delle successive modifiche.

La classificazione, necessaria e fondamentale, è prodromica all'inserzione di un documento all'interno di un determinato fascicolo.

3.1.4. Processo di gestione - Fascicolazione

La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla relativa pratica.

[18] Nel caso di dubbi in merito alla voce del titolario da attribuire al documento, l'operatore addetto al protocollo si confronta con il Responsabile della gestione documentale in merito alla corretta classificazione.

Firmato digitalmente da Frighetto Iole Antonella

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza sotto-fascicolo, secondo l'ordine cronologico di registrazione.

I fascicoli sono organizzati per[19]:

- **affare**, al cui interno vengono compresi documenti relativi a una competenza non proceduralizzata, ma che, nella consuetudine amministrativa, l'Istituzione scolastica deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta. Esso, infatti, viene chiuso alla chiusura dell'affare;
- **attività**, al cui interno vengono compresi i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;
- **persona fisica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **persona giuridica**, al cui interno vengono compresi tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni;
- **procedimento amministrativo**, al cui interno vengono conservati una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo. Il fascicolo viene chiuso al termine del procedimento amministrativo[20].

All'interno dei fascicoli è possibile creare dei sotto-fascicoli.

Ogni ufficio si fa carico di gestire le pratiche di propria competenza. Qualora un documento dia luogo all'avvio di un nuovo procedimento, il soggetto preposto provvede all'apertura di un nuovo fascicolo. Al fine di determinare la tipologia di aggregazione documentale (tipologia di serie e tipologia di fascicoli) da adottare, si fa riferimento al Piano di organizzazione delle aggregazioni documentali, riportato all'Allegato in allegato (7.3). Un documento può essere assegnato anche a più fascicoli. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "**apertura**" che comprende la registrazione di alcune informazioni essenziali. Il fascicolo informatico, infatti, reca l'indicazione[21]:

- dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'identificativo del fascicolo medesimo.

[19] Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[20] A norma dell'art. 41, comma 2, del CAD, "*La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati;* […]".
[21] A norma dell'art. 41, comma 2-*ter*, del CAD.

Firmato digitalmente da Frighetto Iole Antonella

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. In alcuni casi, è possibile utilizzare anche il primo livello (titolo), come per i fascicoli di persona fisica.

In presenza di un documento da inserire in un fascicolo, i soggetti deputati alla fascicolazione stabiliscono, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un procedimento in corso, oppure se dà avvio ad un nuovo procedimento:

1. se si colloca nell'ambito di un procedimento in corso:
    - selezionano il relativo fascicolo;
    - collegano la registrazione di protocollo del documento al fascicolo selezionato (se si tratta di un documento su supporto cartaceo, assicurano l'inserimento fisico dello stesso nel relativo carteggio);
2. se dà avvio ad un nuovo procedimento:
    - eseguono l'operazione di apertura del fascicolo di cui al paragrafo precedente;
    - assegnano la pratica su indicazione del responsabile del procedimento;
    - collegano la registrazione di protocollo del documento al fascicolo aperto.

Il fascicolo viene chiuso al termine del procedimento. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Quando si verifica un errore nella assegnazione di un fascicolo, l'utente abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza. Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora dell'operazione.

I fascicoli sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli, ripartito per ciascun titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli. La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che la scuola può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività. Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe ed eventuale sottoclasse);
- il numero di fascicolo (ed altre eventuali partizioni in sotto-fascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sotto-fascicoli e inserti);
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio di storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

Oltre ad essere inserito in un fascicolo, un documento può essere inserito in una o più serie documentali, che rappresentano aggregazioni di documenti con caratteristiche omogenee, raggruppati ad esempio in base alla tipologia documentaria (es. delibere, decreti, fatture) o alla

Firmato digitalmente da Frighetto Iole Antonella

provenienza (cioè se prodotti da un medesimo organo, come il Consiglio d'istituto o il Collegio dei docenti) o all'oggetto (es. documenti relativi ad un progetto PON).[22] I documenti all'interno di una serie, non essendo aggregati utilizzando il titolario di classificazione come nel caso dei fascicoli, possono appartenere a titoli e classi differenti tra loro. La serie documentale stessa, quindi, non viene classificata in base alle partizioni del titolario.

Specifiche indicazioni in merito alle modalità di inserimento dei documenti nelle aggregazioni documentali, sono contenute nell'Appendice "*Focus sulle aggregazioni documentali delle Istituzioni scolastiche*" alle "Linee guida per la gestione documentale nelle Istituzioni scolastiche".

3.1.5. Processo di gestione - Archiviazione

Le Istituzioni scolastiche definiscono nel proprio manuale la gestione degli archivi rifacendosi alla seguente articolazione archivistica[23]:

- **archivio corrente**: riguarda i documenti necessari alle attività correnti;
- **archivio di deposito**: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- **archivio storico**: riguarda i documenti storici selezionati per la conservazione permanente.

L'archiviazione, per alcune fattispecie di documenti, può avvenire presso archivi gestiti a livello centrale dal Ministero dell'Istruzione. A titolo esemplificativo, le istanze che pervengono alla scuola mediante il Servizio Istanze OnLine, che permette di effettuare in modalità digitale la presentazione delle domande connesse ai principali procedimenti amministrativi dell'Amministrazione, sono protocollate in ingresso dalla AOO appositamente costituita presso il Ministero dell'Istruzione, e sono rese disponibili alle Istituzioni scolastiche.

Tenendo conto che l'archivio corrente è organizzato su base annuale e che il passaggio dall'archivio corrente all'archivio di deposito è possibile solo qualora il fascicolo contenga documenti afferenti a procedimenti conclusi, è necessario verificare quali fascicoli contengono documenti afferenti ad una pratica chiusa. Tale verifica può essere effettuata:

- ad ogni fine anno, in modo tale che i fascicoli delle pratiche non chiuse entro il dicembre precedente vengano "trascinati" nell'archivio corrente del nuovo anno e i fascicoli delle pratiche chiuse vengano "trascinati" nell'archivio di deposito;

oppure,

- in corso d'anno qualora la pratica sia chiusa.

Dato che sarebbe troppo oneroso e pressoché inutile conservare illimitatamente l'archivio nella sua totalità esso deve essere periodicamente sottoposto ad una selezione razionale, che va prevista fin dal momento della creazione dei documenti, e va disciplinata nel piano di conservazione[24], a sua volta integrato con il sistema di classificazione. A tal fine si inserisce lo sfoltimento (attività eseguita nell'archivio corrente).

---

[22] Tale definizione di "serie documentale" è basata sul paragrafo 4 dell'Allegato 5 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[23] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[24] Art. 68, comma 1, del D.P.R. 445/2000.

Firmato digitalmente da Frighetto Iole Antonella

Lo sfoltimento è un'attività propedeutica ad una corretta conservazione documentale: al momento della chiusura del fascicolo, ad esempio, oppure prima del trasferimento dello stesso all'archivio di deposito, l'eventuale carteggio di carattere transitorio e strumentale deve essere selezionato ed estratto dal fascicolo da parte dell'operatore incaricato del trattamento della pratica. Si tratta, cioè, di estrarre dal fascicolo le copie e i documenti che hanno appunto carattere strumentale e transitorio, utilizzati dall'operatore incaricato o dal responsabile del procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad es., appunti, promemoria, copie di normativa e documenti di carattere generale).

Nell'ambito dell'archivio di deposito avviene l'operazione di scarto che non deve essere applicato, salvo diverse indicazioni dettate dalla Soprintendenza archivistica, su documentazione facente parte dell'archivio storico le cui pratiche siano esaurite da oltre 40 anni, mentre può essere sempre effettuato sulla documentazione dell'archivio di deposito, che contiene tutte le pratiche chiuse che non abbiano maturato i 40 anni di conservazione.

La carenza di spazio negli archivi nonché la produzione smisurata e la conservazione di carte anche inutili non possono giustificare la distruzione non autorizzata di documenti e nemmeno la cancellazione di documenti elettronici[25], poiché lo scarto dei documenti dell'archivio della scuola è subordinato all'autorizzazione della Soprintendenza archivistica[26]. È una forma di scarto anche la cancellazione di documenti elettronici.

Fatto salvo quanto sopra, l'operazione di scarto è supportata dal massimario di conservazione e scarto, grazie al quale è prodotto annualmente l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico. I documenti selezionati per la conservazione permanente sono depositati contestualmente agli strumenti che ne garantiscono l'accesso nell'Archivio di Stato competente per territorio o trasferiti nella separata sezione di archivio, secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

3.2. Processo di conservazione

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di conservazione che è coerente con quanto disposto dal CAD e dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Il processo di conservazione prevede quattro fasi:

- versamento in archivio di deposito;
- scarto;
- versamento in archivio storico;
- delocalizzazione.

In questo contesto, si inserisce la figura del Responsabile della conservazione, i cui compiti sono stati descritti al precedente paragrafo 2.2.

[25] Art. 169, D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".
[26] Art. 21, comma 1, D.Lgs. 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137".

Firmato digitalmente da Frighetto Iole Antonella

Ai sensi dell'art. 34, comma 1-*bis*, del CAD, come modificato dall'art. 25, comma 1, lett. e), del D.L. 76/2020 (c.d. "Decreto Semplificazione"), convertito con Legge n. 120/2020, le Pubbliche Amministrazioni possono procedere alla conservazione dei documenti informatici:

a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID[27], avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

Per la conservazione dei documenti informatici, l'Istituzione scolastica si avvale del modello esterno del servizio del Conservatore accreditato Aruba S.p.A.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Ai sensi dell'art. 44, comma 1-*ter*, del CAD, come da ultimo modificato dal D.L. 76/2020, "*In tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida*".

In ogni caso, i sistemi di conservazione devono consentire la possibilità di eliminare i documenti ove necessario (laddove previsto dalla normativa vigente).

Si tenga conto altresì del periodo di conservazione e di scarto dei documenti che contengono al loro interno dati personali. In base alla normativa vigente in materia di protezione dei dati personali, infatti, tale periodo di tempo non deve essere superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

3.2.1. VERSAMENTO IN ARCHIVIO DI DEPOSITO

Nella fase di versamento in archivio di deposito[28] il responsabile per la tenuta degli archivi[29]:

---

[27] L'AgID ha adottato con Determinazione n. 455/2021 il "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*" e i relativi allegati. L'allegato A, in particolare, fissa i requisiti per l'erogazione del servizio di conservazione per conto delle Pubbliche Amministrazioni. Il regolamento prevede, inoltre, l'istituzione di un *marketplace* per i servizi di conservazione quale sezione autonoma del *Cloud Marketplace* cui possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle Pubbliche Amministrazioni. L'iscrizione al *marketplace* non è obbligatoria ma i conservatori che intendono partecipare a procedure di affidamento da parte delle Pubbliche Amministrazioni devono ugualmente possedere i requisiti previsti nel suddetto regolamento e sono sottoposti all'attività di vigilanza di AgID.

[28] L'art. 67 del D.P.R. 445/2000 disciplina il trasferimento dei documenti all'archivio di deposito, prevedendo, nel dettaglio che "*1. Almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito costituito presso ciascuna amministrazione. 2. Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. 3. Il responsabile del servizio per la gestione*

Firmato digitalmente da Frighetto Iole Antonella

- controlla periodicamente tutte le pratiche fascicolate presenti nell'archivio corrente, sia cartaceo che elettronico, al fine di identificare quelle per cui la lavorazione è già stata conclusa e compila una lista della documentazione presente nelle pratiche chiuse;
- provvede allo sfoltimento eliminando l'eventuale carteggio di carattere transitorio e strumentale presente nel fascicolo;
- provvede al versamento di tutta la documentazione, sia cartacea che elettronica, presente nella lista all'archivio di deposito;
- provvede al versamento nell'archivio corrente del nuovo anno della documentazione delle pratiche appartenenti alle pratiche presenti nell'archivio corrente (ancora in fase di lavorazione).

Di seguito, si fornisce la rappresentazione grafica del processo sopra descritto.

3.2.2. Scarto

Nell'archivio di deposito si eseguono le attività relative alla fase di scarto in cui il responsabile per la tenuta degli archivi:

- verifica periodicamente la tipologia e i tempi di conservazione della documentazione, sia cartacea che elettronica, presente nell'archivio di deposito per individuare quella da scartare applicando le disposizioni del massimario di conservazione e scarto;
- procede con la compilazione di una lista della documentazione da scartare e da inviare alla Soprintendenza per l'approvazione e la comunica al Responsabile della gestione documentale;
- invia, in caso di documenti cartacei, la documentazione presente sulla lista al soggetto competente per la distruzione della carta;
- provvede ad eliminare la documentazione elettronica presente nella lista approvata dalla Soprintendenza.

In caso di affidamento esterno del servizio di conservazione, l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al Responsabile della conservazione che, a sua volta,

---

dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.".

[29] Il responsabile per la tenuta degli archivi può essere il Dirigente Scolastico o altro personale in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del D.P.R. 28 dicembre 2000, n. 445.

Firmato digitalmente da Frighetto Iole Antonella

verificato il rispetto dei termini temporali stabiliti dal massimario di conservazione e scarto, lo comunica al Responsabile della gestione documentale.

3.2.3. VERSAMENTO IN ARCHIVIO STORICO

Nella fase di versamento in archivio storico[30], il responsabile per la tenuta degli archivi:

- verifica se nell'archivio di deposito esistono pratiche esaurite da oltre 40 anni, sia in forma cartacea che elettronica;
- provvede a preparare una lista contenente tutta la documentazione presente nelle pratiche stesse, qualora dovessero essere presenti pratiche esaurite da oltre 40 anni;
- provvede ad inviare la lista della documentazione da versare al personale competente, in caso di documentazione cartacea, che deve individuare un archivio storico con sufficiente spazio per dare seguito al versamento.

3.2.4. DELOCALIZZAZIONE

La fase di delocalizzazione è avviata nel caso in cui, dopo aver effettuato le operazioni di scarto e dopo aver effettuato l'eventuale versamento nell'archivio storico, dalla verifica del grado di saturazione dell'archivio di deposito cartaceo, risulta che l'archivio è saturo. Nel caso in cui l'archivio di deposito cartaceo dovesse essere saturo, il responsabile per la tenuta degli archivi:

- provvede ad individuare la documentazione da delocalizzare selezionandola tra quella più prossima alla data di scarto;
- provvede a stilare la lista dei documenti da delocalizzare.

L'addetto competente:

- analizza la documentazione ricevuta;
- provvede a identificare una struttura con sufficiente spazio negli archivi;
- autorizza la delocalizzazione della documentazione presso una struttura interna nel caso in cui questa sia disponibile.

Il responsabile per la tenuta degli archivi provvede ad inviare la richiesta di autorizzazione alla Soprintendenza competente. Una volta ricevuta l'approvazione dalla Soprintendenza competente, il responsabile per la tenuta degli archivi provvede ad inviare la documentazione da delocalizzare.

4. IL DOCUMENTO AMMINISTRATIVO

Per documento amministrativo, ai sensi dell'art. 1, comma 1, lett. a), del D.P.R. 28 dicembre 2000, n. 445, si intende "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*".

[30] L'art. 69 del D.P.R. 445/2000, rubricato "Archivi storici", prevede che "*I documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali*".

Firmato digitalmente da Frighetto Iole Antonella

Nell'ambito del processo di gestione documentale, il documento amministrativo dal punto di vista operativo è classificabile in documento:

- ricevuto;
- inviato;
- di rilevanza esterna;
- di rilevanza interna.

In base alla natura, invece, è classificabile in documento:

- analogico;
- informatico.

L'art. 40, comma 1, del CAD, come modificato da ultimo dall'art. 66, comma 1, del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida*".

Per ciò che concerne la trasmissione dei documenti tra Pubbliche Amministrazioni, ai sensi di quanto disposto dall'art. 47 del CAD, essa deve avvenire:

- attraverso l'utilizzo della posta elettronica[31]; *ovvero*
- in cooperazione applicativa.

Le suddette comunicazioni sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il comma 2, del citato art. 47, stabilisce infatti che "*Ai fini della verifica della provenienza le comunicazioni sono valide se: a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle Linee guida. È in ogni caso esclusa la trasmissione di documenti a mezzo fax; d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*".

Specifiche indicazioni in materia di scambio di documenti amministrativi protocollati tra AOO sono contenute nell'Allegato 6 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*".

4.1. DOCUMENTO RICEVUTO

La corrispondenza in ingresso può essere acquisita dall'Istituzione scolastica con diversi mezzi e modalità in base sia alla modalità di trasmissione scelta dal mittente sia alla natura del documento. Un documento informatico può essere recapitato[32]:

- a mezzo posta elettronica convenzionale (PEO);

[31] Come riportato nell'Appendice C dell'Allegato 6 alle *Linee Guida per la formazione, gestione e conservazione dei documenti informatici*, l'utilizzo della posta elettronica è *"da intendersi quale modalità transitoria nelle more dell'applicazione delle comunicazioni tra AOO tramite cooperazione applicativa"*. Pertanto, la cooperazione applicativa viene identificata come l'unica modalità a tendere per le comunicazioni di documenti amministrativi protocollati tra AOO.

[32] Per ciò che riguarda la trasmissione dei documenti tra le Pubbliche Amministrazioni, specifiche indicazioni sono contenute all'interno dell'art. 47 del CAD.

Firmato digitalmente da Frighetto Iole Antonella

- a mezzo posta elettronica certificata (PEC);
- mediante supporto removibile (ad es. CD, *pendrive*).

Un documento analogico, assunto che le principali tipologie di documenti analogici che pervengono alle Istituzioni scolastiche sono telegrammi, documenti per posta ordinaria e raccomandate, può essere recapitato:

- attraverso il servizio di posta tradizionale;
- *pro manibus*.

I documenti, analogici o digitali, di cui non sia identificabile l'autore sono regolarmente aperti e registrati al protocollo (con indicazione "Mittente anonimo"), salvo diversa valutazione del Dirigente Scolastico, che provvederà ad eventuali accertamenti.

I documenti ricevuti privi di firma ma il cui mittente è comunque chiaramente identificabile, vengono protocollati (con indicazione "Documento non sottoscritto") e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso. Sarà poi compito del responsabile del procedimento valutare, caso per caso, ai fini della sua efficacia riguardo ad un affare o ad un determinato procedimento amministrativo, se il documento privo di firma possa essere ritenuto valido o meno[33].

4.2. Documento inviato

I documenti informatici sono inviati all'indirizzo elettronico dichiarato dai destinatari, abilitato alla ricezione della posta per via telematica.

4.3. Documento di rilevanza esterna

Per documento di rilevanza esterna si intende qualunque documento ricevuto/trasmesso da/a altro Ente o altra persona fisica o giuridica. La gestione è normata dal CAD.

4.4. Documento di rilevanza interna

Per documenti di rilevanza interna si intendono tutti quelli che a qualunque titolo sono scambiati tra UOR o persone dell'Istituzione scolastica stessa.

Possono distinguersi in:

- **comunicazioni informali tra UOR** (documenti di natura prevalentemente informativa): per comunicazioni informali tra unità si intendono gli scambi di informazioni che non hanno valenza giuridico probatoria, né rilevanza ai fini dell'azione amministrativa. Queste comunicazioni avvengono, di norma, tramite PEO e non sono soggette a protocollazione ed archiviazione;
- **scambio di documenti fra UOR** (documenti di natura prevalentemente giuridico-probatoria): per scambio di documenti fra unità si intendono le comunicazioni ufficiali

[33] Per approfondimenti in merito alle tipologie di sottoscrizione elettronica, si veda il par. "4.6.1 - Le firme elettroniche".

Firmato digitalmente da Frighetto Iole Antonella

di un certo rilievo ai fini dell'azione amministrativa e delle quali si deve tenere traccia. Le comunicazioni di questo genere devono comunque essere protocollate.

4.5. DOCUMENTO ANALOGICO

Per documento analogico si intende "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*"[34].

Si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa[35].

La sottoscrizione di un documento determina:

- l'**identificazione dell'autore** del documento;
- la **paternità** del documento: con la sottoscrizione l'autore del documento si assume la paternità dello stesso, anche in relazione al suo contenuto. A questo proposito si parla di non ripudiabilità del documento sottoscritto;
- l'**integrità** del documento: il documento scritto e sottoscritto manualmente garantisce da alterazioni materiali da parte di persone diverse da quella che lo ha posto in essere.

4.6. DOCUMENTO INFORMATICO

Per documento informatico si intende "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*"[36]. Il documento informatico, come precisato nel paragrafo 2.1.1. delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate da AgID, è formato mediante una delle seguenti modalità:

"*a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;*

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica".

---

[34] Art. 1, comma 1, lett. p-*bis*), D.lgs. 7 marzo 2005, n. 82, CAD.

[35] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto".

[36] Art. 1, comma 1, lett. p), D.lgs. 7 marzo 2005, n. 82, CAD. La definizione è altresì contenuta all'interno dell'art. 1, comma 1, lett. b), del D.P.R. 445/2000: "*b) DOCUMENTO INFORMATICO: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.*".

Firmato digitalmente da Frighetto Iole Antonella

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

A seconda che il documento informatico sia formato secondo una delle modalità sopra riportate, l'immodificabilità e l'integrità sono garantite da una o più delle operazioni indicate nelle citate Linee Guida, al paragrafo 2.1.1. (pag. 13).

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati associati dall'Istituzione scolastica ai documenti informatici e ai documenti amministrativi informatici corrispondono a quelli obbligatori previsti nell'Allegato 5 delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*". Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici, come i documenti soggetti a registrazione particolare.

Un documento nativo informatico non può essere convertito in formato analogico prima della sua eventuale acquisizione a sistema di protocollo o archiviazione informatica. Nel caso di documenti soggetti a sottoscrizione, è possibile fare ricorso alla firma elettronica avanzata (FEA), messa a disposizione delle Istituzioni scolastiche dal Ministero. I Dirigenti Scolastici ed i Direttori dei Servizi Generali ed Amministrativi delle Istituzioni Scolastiche statali di ogni ordine e grado possono, inoltre, fare ricorso alla firma digitale, tramite l'apposita funzione presente sul SIDI. Le suddette modalità di firma vengono delineate ed analizzate nel paragrafo successivo.

4.6.1. LE FIRME ELETTRONICHE

La firma elettronica costituisce la modalità ordinaria di firma dei documenti informatici.

In particolare, la normativa vigente in materia individua diverse tipologie di sottoscrizione elettronica:

- firma elettronica, ovvero l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzata come metodo di autentificazione (art. 3, n. 10, Reg. UE n. 910/2014);
- firma elettronica avanzata, ovvero l'insieme dei dati allegati o connessi ad un documento informatico che consentono l'identificazione del firmatario e garantiscono la connessione univoca con quest'ultimo (art. 3, n. 11, Reg. UE n. 910/2014);
- firma elettronica qualificata, ovvero una firma elettronica avanzata che si basa su un certificato qualificato (art. 3, n. 12, Reg. UE n. 910/2014);
- firma digitale, ovvero una particolare firma elettronica qualificata che si basa su un certificato qualificato e su un sistema di chiavi crittografiche (art. 1, comma 1, lett. s), CAD).

In considerazione del tipo di tecnologia utilizzata, la firma digitale rappresenta la tipologia di firma più sicura. Essa è disciplinata dall'art. 24 del CAD il quale, ai commi 1, 2, 3 e 4, prevede che "*1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. 2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente. 3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di*

Firmato digitalmente da Frighetto Iole Antonella

validità ovvero non risulti revocato o sospeso. 4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma".

Si tenga conto, altresì, che secondo quanto stabilito dall'art. 24, comma 4-*bis*, del CAD, qualora ad un documento informatico sia apposta una firma digitale o un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso, il documento si ha come non sottoscritto, salvo che lo stato di sospensione sia stato annullato. Ad ogni modo, l'eventuale revoca o sospensione, comunque motivata, ha effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

Si rappresenta, inoltre, che l'articolo 20, comma 1-*bis*, del CAD, come modificato dall'art. 20, comma 1, lett. a) del D.Lgs. 13 dicembre 2017, n. 217, stabilisce che "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida*".

Ai sensi dell'art. 20, commi 1-*ter* e 1-*quater*, del CAD, introdotti dall'art. 20, comma 1, lett. b), del D.lgs. 13 dicembre 2017, n. 217: "(1-*ter*) *L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria. (1-quater) Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico*".

Dalle disposizioni sopra riportate, risulta possibile individuare quale sia l'efficacia probatoria del documento informatico, sulla base del tipo di firma apposta sullo stesso. Nel dettaglio:

- i **documenti sottoscritti con firma elettronica "semplice"** soddisfano il requisito della forma scritta e il loro valore probatorio è liberamente valutabile in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità della firma stessa;
- i **documenti sottoscritti con firma elettronica avanzata, firma elettronica qualificata e firma digitale** soddisfano il requisito della forma scritta e hanno l'efficacia prevista dall'art. 2702 c.c.[37], ovvero fanno piena prova fino a querela di falso;

[37] L'art. 2702 c.c. stabilisce che "*La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta*".

Firmato digitalmente da Frighetto Iole Antonella

- i **documenti sottoscritti con firma digitale con certificato revocato, scaduto o sospeso** fanno piena prova fino a disconoscimento, ai sensi di quanto disposto dall'art. 2712 c.c.[38].

Si rileva, inoltre, che l'art. 25 del CAD, rubricato "*Firma autenticata*", prevede che la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata, autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato, si ha per riconosciuta ai sensi dell'art. 2703 c.c.[39].

Il CAD[40] stabilisce, altresì, che gli atti elencati ai numeri da 1 a 12 dell'art. 1350 c.c. debbano essere sottoscritti con firma elettronica qualificata o digitale, a pena di nullità. Gli atti di cui al n. 13, del citato art. 1350 c.c., invece, oltre ai tipi di firma sopra menzionati, possono essere sottoscritti anche con firma elettronica avanzata o devono essere formati con le ulteriori modalità di cui all'articolo 20, comma 1-*bis*, primo periodo.[41]

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore di protocollo ha verificato la validità della firma digitale con apposita funzione sul sistema di protocollo.

Fatto salvo quanto sopra rappresentato, i documenti informatici possono essere anche senza firma e in tal caso si seguirà la disciplina contenuta al par. "4.1. – Documento ricevuto"[42].

Da ultimo, si rappresenta che, in tutti gli atti cartacei che provengono e che sono generati da sistemi automatizzati, la firma sul documento cartaceo del funzionario responsabile può essere sostituita dalla dicitura dalla "*Firma autografa sostituita a mezzo stampa, ai sensi dell'art. 3, comma 2, Legge 39/1993*".

4.7. CONTENUTI MINIMI DEI DOCUMENTI

Occorre che i documenti amministrativi, sia analogici che informatici, aventi rilevanza esterna, contengano le seguenti informazioni:

- denominazione e logo dell'amministrazione mittente;

---

[38] L'art. 2712 c.c. stabilisce che "*Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".

[39] L'art. 2703 c.c. stabilisce che "*1. Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. 2. L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive*".

[40] Art. 21, comma 2-*bis*, del CAD.

[41] L'art. 1350 c.c. stabilisce che "*Devono farsi per atto pubblico o per scrittura privata, sotto pena di nullità: 1) i contratti che trasferiscono la proprietà di beni immobili; 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta; 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti; 4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione; 5) gli atti di rinunzia ai diritti indicati dai numeri precedenti; 6) i contratti di affrancazione del fondo enfiteutico; 7) i contratti di anticresi; 8) i contratti di locazione di beni immobili per una durata superiore a nove anni; 9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato; 10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato; 11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari; 12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti; 13) gli altri atti specialmente indicati dalla legge*".

[42] Per approfondimenti in merito alla ricezione di documenti privi di firma, si veda il par. "4.1. – Documento ricevuto"

Firmato digitalmente da Frighetto Iole Antonella

- indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- indirizzo di posta elettronica certificata dell'Istituzione scolastica;
- indicazione dell'Istituzione scolastica e dell'UOR che ha prodotto il documento;
- il numero di telefono dell'UOR e del RUP (facoltativo, a piè di pagina se previsto);
- C.F., P.IVA, Codice iPA, Codice univoco per la F.E.

Inoltre, il documento deve recare almeno le seguenti informazioni:

- luogo e data (gg/mm/anno) di redazione del documento;
- numero di protocollo;
- oggetto del documento.

Esso non deve contenere il riferimento al numero di fax, coerentemente a quanto disposto dall'art. 14, comma 1-*bis*, del decreto-legge 21 giugno 2013, n. 69, così come modificato dalla legge 9 agosto 2013, n. 98, recante "*Misure per favorire la diffusione del domicilio digitale*", il quale stabilisce che, ai fini della verifica della provenienza delle comunicazioni, è in ogni caso esclusa la trasmissione di documenti a mezzo fax tra Pubbliche Amministrazioni. È facoltà del Responsabile della gestione documentale aggiungere a quelle fin qui esposte altre regole per la determinazione dei contenuti e per la definizione della struttura dei documenti informatici. Si evidenzia, altresì, che in tema di accesso ai documenti amministrativi[43], a ciascuna Istituzione scolastica spetta l'onere di specificare con precisione gli estremi di registrazione di un documento sui propri sistemi di protocollo.

L'indicazione di tali elementi (tra cui l'oggetto) deve essere rispondente agli *standard* indicati nel presente manuale[44]. Ciò perché prerequisito essenziale del pieno godimento del diritto all'accesso agli atti è la reperibilità di quest'ultimi che è assicurata da una corretta e standardizzata definizione/trascrizione dell'oggetto.

4.8. PROTOCOLLABILITÀ DI UN DOCUMENTO

Sono oggetto di registrazione obbligatoria, ai sensi dell'art. 53, comma 5, del D.P.R. n. 445 del 2000, i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici[45].

Inoltre, l'art. 40-*bis* del CAD, come modificato dagli artt. 37, comma 1, e 66, comma 1, del D.lgs. 13 dicembre 2017, n. 217, prevede che formano oggetto di registrazione di protocollo ai sensi dell'articolo 53[46] del D.P.R. n. 445 del 2000, "*le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida*".

---

[43] Nell'ambito della disciplina di accesso, l'art. 1, comma 1, lett. d), della L. 241/1990 definisce il documento amministrativo come "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*".

[44] Per ulteriori approfondimenti, si veda il par. "5.2. - Scrittura di dati di protocollo".

[45] Le *"Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, emanate dall'AgID, prevedono che "*La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53, comma 5, del TUDA*".

[46] L'art. 53, comma 5, del D.P.R. 445/2000, al primo periodo prevede che "*Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici*".

Firmato digitalmente da Frighetto Iole Antonella

Sono invece esclusi dalla registrazione obbligatoria[47]:

- le gazzette ufficiali;
- i bollettini ufficiali e i notiziari della Pubblica Amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste;
- i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

Nel caso in cui sia necessario attribuire una data certa a un documento informatico non soggetto a protocollazione prodotto all'interno dell'Istituzione scolastica, si applicano le regole per la "validazione temporale" di cui al DPCM del 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*".

In particolare, la "validazione temporale" consente di stabilire il momento temporale in cui il documento informatico è stato formato ed è definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile a terzi.

Lo strumento per ottenere questo risultato è la "marca temporale"[48], ovvero "*il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo*".

5. IL PROTOCOLLO INFORMATICO

5.1. PROTOCOLLAZIONE

Per protocollazione si intende l'attività di registrazione di protocollo mediante la quale è eseguita l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

I documenti che devono essere registrati a protocollo sono indicati nel paragrafo "4.8. - Protocollabilità di un documento amministrativo".

Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immodificabile. Quindi non è consentito:

- protocollare un documento già protocollato;
- apporre manualmente la segnatura di protocollo, salvo i casi in cui l'apposizione tramite l'applicativo possa deteriorare le informazioni fondamentali del documento (ad es.

[47] Art. 53, comma 5, del D.P.R.445/2000.
[48] Art. 1, comma 1, del DPCM 22 febbraio 2013.

Firmato digitalmente da Frighetto Iole Antonella

sovrapposizione del timbro in ingresso al timbro in uscita, presenza di etichetta adesiva plastificata che verrebbe annerita dalla stampante);

- in caso di spedizione ed arrivi massivi, apporre una segnatura del tipo es.: 1741/1, 1741/2, 1741/3, ecc. oppure attribuire ad essi lo stesso numero di protocollo;
- protocollare sul registro ufficiale atti di rilevanza interna senza utilizzare l'apposita modalità di protocollazione interna;
- selezionare un numero di protocollo alla data di ricezione del documento al fine di effettuare l'operazione di protocollazione in una data successiva;
- apporre la firma sul documento successivamente alla protocollazione;
- associare ad una precedente registrazione ulteriori allegati prodotti o ricevuti successivamente.

La protocollazione per ogni documento è effettuata mediante la memorizzazione dei seguenti elementi[49]:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari, in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- informazioni inerenti all'assegnazione interna all'amministrazione e la eventuale classificazione[50].

L'operazione di protocollazione, così come appena descritta, deve essere effettuata solo **dopo** aver caricato sul sistema il documento principale e i suoi allegati (che devono riportare tutti il medesimo numero di protocollo).

5.2. Scrittura di dati di protocollo

La gestione informatizzata dei flussi documentali dell'Istituzione scolastica necessita una particolare attenzione alla qualità delle informazioni associate, in fase di protocollazione, ai documenti interessati, al fine di evitare che questi risultino non reperibili o difficilmente rintracciabili.

A tal fine, sono di seguito riportate le regole cui gli utilizzatori del sistema di protocollo informatico devono attenersi, per la redazione dei seguenti dati:

[49] Tali elementi sono definiti nell'art. 53, comma 1, del D.P.R. 445/2000.
[50] Tale elemento è previsto dalle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.

Firmato digitalmente da Frighetto Iole Antonella

TIPO DI DATI	REGOLE
Nomi di persona	- Prima il nome e poi il cognome - Tutto maiuscolo **Esempio**: MARIO ROSSI
Titoli professionali e/o istituzionali	Sempre omessi
Nomi di città e di stati	In lingua italiana, per esteso e senza puntare **Esempio**: San Vitaliano (Na) e non S. Vitaliano (Na)
Nomi di ditte e società	- Se riportano nomi di persona valgono le precedenti regole - Usare sigle, in maiuscolo e senza punti o, in alternativa, acronimi - La forma societaria senza punti **Esempio**: GIUSEPPE BIANCO, ACME SpA
Enti e associazioni in genere	Usare sigle in maiuscolo e senza punti, laddove disponibili
Ministeri	Usare la forma ridotta e puntata della sola parola Ministero, oppure l'acronimo **Esempio**: MIN. ISTRUZIONE, oppure MI
Enti di secondo livello	Usare la forma estesa o acronimi noti
Sigle in genere	In maiuscolo e senza punti **Esempio**: MI
Virgolette e apici	- Digitare il carattere direttamente dalla tastiera - Non eseguire la funzione copia e incolla di *Windows*
Date	Usare il seguente formato numerico: GG-MM-AAAA o GGMMAAAA **Esempio**: 20-07-2020 o 20072020 e non 20/07/2020

Oltre a quanto sopra rappresentato, l'Istituzione scolastica adotta le seguenti ulteriori regole per la redazione dei dati: [*elenco regole aggiuntive*].

5.3. Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. L'operazione di segnatura è effettuata dall'applicativo automaticamente e contemporaneamente all'operazione di registrazione di protocollo[51]. Essa consente di individuare ciascun documento in modo inequivocabile.

[51] Art. 55, comma 2, D.P.R. 445/2000 e "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID, pag. 20.

Firmato digitalmente da Frighetto Iole Antonella

Le informazioni minime previste nella segnatura di protocollo sono[52]:

- il progressivo di protocollo[53];
- la data di protocollo;
- l'identificazione in forma sintetica dell'Amministrazione o dell'Area Organizzativa individuata.

L'operazione di segnatura di protocollo può includere ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo. Quando il documento è indirizzato ad altre Amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

La segnatura di protocollo dell'Istituzione scolastica, in ottemperanza alle regole tecniche precedentemente esposte, adotta il *set* di informazioni minime ed utilizza quale identificativo dell'Amministrazione il codice con cui l'Istituzione scolastica è univocamente identificata sull'indice delle Pubbliche Amministrazioni.

5.4. Differimento della registrazione di protocollo

Le registrazioni di protocollo dei documenti pervenuti all'Istituzione scolastica sono effettuate nella giornata di arrivo e comunque non oltre tre giorni lavorativi dal ricevimento di detti documenti. Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo, il Responsabile della gestione può autorizzare la registrazione in tempi successivi fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo, esplicitandone l'autorizzazione attraverso apposite note interne. Il protocollo differito consiste nel differimento dei termini di registrazione e si applica ai documenti in arrivo.

5.5. Ricevuta di avvenuta protocollazione

La ricezione dei documenti via PEC comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, una al servizio di protocollazione informatica. Nel caso di ricezione di documenti informatici mediante PEC, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata, utilizzato dall'Istituzione scolastica con gli *standard* specifici.

In caso di documenti pervenuti via PEO, è inviata una conferma di ricezione con relativa segnatura informatica in formato XML del documento attraverso apposita funzione ("Inoltro" o "Rispondi").

5.6. Registro giornaliero di protocollo

Il registro di protocollo è lo strumento attraverso cui è possibile identificare in modo univoco e certo i documenti ricevuti e spediti mediante la registrazione di determinati elementi che caratterizzano ogni singolo documento. Per tale motivo, il registro di protocollo svolge una

[52] Tali informazioni sono definite all'art. 55 del D.P.R. 445/2000.

[53] Ai sensi dell'art. 57, comma 1, del D.P.R. 445/2000 44 "*Il numero di protocollo è progressivo e costituito da almeno sette cifre numeriche. La numerazione è rinnovata ogni anno solare*.".

Firmato digitalmente da Frighetto Iole Antonella

fondamentale funzione giuridico probatoria, attestando l'esistenza di un determinato documento all'interno del sistema di gestione documentale e garantendone l'autenticità.

Dunque, in coerenza con la normativa vigente, il registro ufficiale di protocollo è unico, sia per la protocollazione in ingresso, che in uscita, che in modalità interna e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo adottato. La numerazione si chiude al 31 dicembre e ricomincia il 1° gennaio successivo. Essa si aggiorna automaticamente e quotidianamente.

Deve essere prodotto automaticamente il registro giornaliero di protocollo costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Esso deve essere inviato automaticamente dal sistema di protocollo, in formato tale da garantirne la non modificabilità. Al fine di garantire la non modificabilità delle operazioni di registrazione, il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione[54].

Si specifica che con riferimento alle protocollazioni effettuate esclusivamente sul Registro ufficiale di protocollo, l'operatore che gestisce lo smistamento dei documenti può definire "riservata" una registrazione di protocollo ed assegnarla per competenza ad un utente assegnatario.

Si ricorda che sono soggetti a protocollazione riservata i seguenti documenti:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico o di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa.

È possibile impostare una data di scadenza al carattere riservato del documento. Una volta scaduti i termini di riservatezza, il documento diventa visibile a chi è abilitato.

5.7. REGISTRO DI EMERGENZA

Nel caso di interruzioni del funzionamento del sistema di protocollo informatico per cause tecniche accidentali o programmate, ai sensi dell'art. 63 del Testo Unico, le registrazioni di protocollo vengono effettuate su un registro di emergenza[55].

---

[54] "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*", emanate dall'AgID.

[55] L'art. 63 del D.P.R. 445/2000 prevede che "*1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in*

Firmato digitalmente da Frighetto Iole Antonella

Il Responsabile della gestione documentale autorizza con proprio provvedimento la predisposizione del registro di emergenza in forma cartacea oppure in forma digitale e, al ripristino della funzionalità del sistema di protocollo informatico, tutte le registrazioni effettuate vengono inserite a sistema, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza, mantenendo una correlazione con il numero utilizzato in emergenza. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema di protocollo. In questi casi, dovranno essere compilati in ogni loro parte e firmati, i Moduli di Registrazione di Emergenza.

Qualora l'interruzione del funzionamento del sistema di protocollo si prolunghi per più di ventiquattro ore, il Responsabile della gestione documentale, ai sensi della normativa vigente, autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle informazioni di cui sopra, vengono riportati gli estremi del provvedimento di autorizzazione.

5.8. REGISTRI PARTICOLARI

All'interno dell'Istituzione scolastica sono istituiti registri particolari che possono essere sottratti alla consultazione da parte di chi non sia espressamente abilitato e per i quali possono essere previste particolari forme di riservatezza e di accesso. Su questi registri vanno caricati solo i documenti informatici o le immagini dei documenti cartacei secondo le istruzioni presenti sul decreto istitutivo del registro particolare in parola che deve essere integralmente riportato nel presente manuale.

I documenti che sono soggetti a particolare registrazione dell'Istituzione scolastica e che, ai sensi dell'art. 53, comma 5, del D.P.R. 445/2000, sono esclusi dalla protocollazione, sono definiti nel presente manuale, con indicazione della modalità di gestione dei relativi registri.

Sono soggetti a registrazione particolare i documenti indicati nell'apposito allegato (7.4).

Per la gestione del trattamento delle registrazioni particolari informatiche vengono individuati i seguenti registri indicati nell'apposito allegato con le relative modalità di gestione (7.5).

5.9. ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO

La necessità di modificare anche un solo campo tra quelli obbligatori della registrazione di protocollo registrato in forma non modificabile, per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Solo il Responsabile della gestione documentale è autorizzato ad annullare ovvero a dare disposizioni di annullamento delle registrazioni di protocollo. L'annullamento di una registrazione di protocollo deve essere richiesto con specifica e-mail, adeguatamente motivata,

---

emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".

Firmato digitalmente da Frighetto Iole Antonella

indirizzata al Responsabile della gestione documentale che, solo a seguito della valutazione della particolare questione, può autorizzare l'annullamento stesso.

Le informazioni annullate devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. In tale ipotesi, la procedura per indicare l'annullamento riporta la dicitura "annullato" in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione. Il sistema registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Al momento dell'annullamento di una registrazione di protocollo generale l'applicativo richiede la motivazione e gli estremi del provvedimento di annullamento.

5.10. MODALITÀ DI SVOLGIMENTO DEL PROCESSO DI SCANSIONE

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico *file* in un formato *standard* abilitato alla conservazione;
- verifica della correttezza dell'acquisizione delle immagini e della esatta corrispondenza delle immagini ottenute con gli originali cartacei;
- collegamento delle immagini alla rispettiva registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

In linea con la certificazione di processo[56], l'operatore di protocollo, a valle del processo di scansione, attesta la conformità del documento scansionato al documento originale.

In breve, la conformità della copia per immagine su supporto informatico di un documento analogico è garantita mediante:[57]

- attestazione di un pubblico ufficiale;
- apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20, comma 1-*bis*, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

L'attestazione di conformità delle copie può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine.

Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

In ogni caso non vengono riprodotti in formato immagine i documenti che per caratteristiche fisiche non possono essere sottoposti a scansione (formati non *standard* o particolarmente voluminosi).

---

[56] Si vedano, in merito, gli articoli 22, comma 1-*bis*, e 23-*ter*, comma 1-*bis*, del CAD e l'Allegato 3 alle "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" emanate dall'AgID.
[57] Art. 22 del CAD.

Firmato digitalmente da Frighetto Iole Antonella

Si precisa che qualora debbano essere protocollati documenti contenenti categorie particolari di dati personali di cui all'art. 9 del Regolamento UE 679/2016, l'operatore di protocollo, dotato delle necessarie abilitazioni, dovrà contrassegnare il documento come contenente dati riservati[58].

6. ACCESSO, TRASPARENZA E PRIVACY

6.1. TUTELA DEI DATI PERSONALI E MISURE DI SICUREZZA

Il sistema di gestione documentale dell'Istituzione scolastica deve adottare un meccanismo di *compliance* e rispetto della normativa in materia di protezione dei dati personali, ai sensi del Reg. UE 679/2016 e del D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018[59].

L'Istituzione scolastica deve intraprendere iniziative volte ad ottemperare a quanto previsto dal Regolamento UE 679/2016, con particolare riferimento:

- al principio di liceità del trattamento dei dati;
- al principio di minimizzazione del trattamento dei dati[60];
- all'esercizio dei diritti di cui agli artt. 15-22 del GDPR da parte degli interessati;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- all'individuazione del Responsabile della protezione dei dati;
- all'individuazione dei Soggetti autorizzati al trattamento dei dati;
- all'analisi dei rischi sui diritti e le libertà dei soggetti interessati;
- alle misure di sicurezza[61].

Fatto salvo quanto sopra, particolare rilevanza assume il concetto di *accountability* e la capacità di adottare un processo efficace per la protezione dei dati, affinché si riduca al minimo il rischio di una loro possibile violazione.

A tal fine, il Responsabile della gestione documentale, in accordo con il Responsabile della conservazione, con il Responsabile per la transizione digitale, e acquisito il parere del Responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Reg. UE 679/2016, anche in funzione delle tipologie di dati

---

[58] Per ulteriori approfondimenti, si veda il par. "6.1 – Tutela dei dati personali e misure di sicurezza".

[59] *"Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"* emanate dall'AgID, stabiliscono che "[…] *il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.*".

[60] Art. 5, comma 1, lett. c), del Regolamento UE 679/2016.

[61] Le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento; in questo senso l'art. 32 par. 1 del Regolamento UE 679/2016 offre una lista aperta e non esaustiva.

Firmato digitalmente da Frighetto Iole Antonella

trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

Sul punto, il Garante della *privacy* nel Parere sullo schema di "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" del 13 febbraio 2020, ha evidenziato che il mero rinvio alle misure di cui alla circolare AgID del 18 aprile 2017, n. 2/2017, nell'ambito dei requisiti di sicurezza cui sono tenuti i vari soggetti coinvolti nel trattamento, non è di per sé sufficiente ad assicurare l'adozione di misure di sicurezza del trattamento adeguate, in conformità al Regolamento, a norma del quale, occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'Istituzione scolastica è tenuta ad adottare, pertanto, idonee e preventive misure di sicurezza, volte a custodire i dati personali trattati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Nello specifico, le misure di carattere tecnico/organizzativo adottate dall'Istituzione scolastica sono le seguenti riportate in allegato (7.6).

6.2. DIRITTO DI ACCESSO AGLI ATTI

6.2.1. ACCESSO DOCUMENTALE

Per diritto di accesso si intende, ai sensi dell'art. 22, comma 1, lett. a), della L. 241/1990, "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi*".

Gli istanti devono essere portatori di un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento amministrativo e ai documenti connessi.

Gli interessati devono effettuare una richiesta di accesso motivata, essendo necessaria una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso.

Il diritto di accesso è escluso per[62]:

- i documenti coperti dal segreto di Stato;
- i procedimenti tributari;
- l'attività della Pubblica Amministrazione diretta all'emanazione di atti normativi o amministrativi generali;
- i procedimenti selettivi contenenti informazioni di carattere psicoattitudinale.

Il diritto all'accesso ai documenti amministrativi è prioritario rispetto al diritto alla riservatezza in tutti quei casi in cui l'istanza ostensiva sia preordinata alla tutela e alla difesa dei propri interessi giuridici.

[62] Art. 24, L. 241/1990.

Firmato digitalmente da Frighetto Iole Antonella

L'Istituzione scolastica deve effettuare una valutazione oggettiva circa la posizione dell'istante per verificare l'esistenza di un nesso di strumentalità rispetto ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso, tenendo conto altresì di quanto previsto eventualmente nello specifico regolamento per l'accesso documentale, adottato dalla scuola, in conformità alle previsioni contenute nella delibera ANAC 1309/2016.

Per quanto afferisce ai profili *privacy*, il D.Lgs. 196/2003 all'art. 59, rubricato "*Accesso a documenti amministrativi e accesso civico*" prevede che "*1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.*".

In breve, si rileva che rispetto ai[63]*:*

- *Dati personali:* il diritto all'accesso ai documenti amministrativi può prevalere sull'interesse alla riservatezza, nel rispetto del principio di minimizzazione;
- *Dati cc.dd. sensibili e giudiziari:* il diritto all'accesso prevale solo laddove sia strettamente indispensabile;
- *Dati cc.dd. sensibilissimi (dati genetici e/o idonei a rivelare lo stato di salute e la vita sessuale):* il diritto di accesso prevale esclusivamente se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

A tal proposito, nella gestione degli accessi e consultazione dei documenti detenuti dall'Istituzione scolastica, da parte di terzi, il Responsabile della gestione è tenuto ad informare in modo costante ed aggiornato il Responsabile della protezione dei dati personali.

In ogni caso, nell'ipotesi di accesso diretto ai propri archivi, l'Amministrazione titolare dei dati, rilascia all'Amministrazione procedente apposita autorizzazione in cui vengono indicati eventuali limiti e condizioni di accesso, volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente anche mediante la stipula di apposite convenzioni di servizio.

Allo stesso modo, nel caso in cui sia effettuata una protocollazione riservata (come indicato nel paragrafo 5.8.), la visibilità completa del documento è possibile solo all'utente assegnatario per competenza e agli operatori di protocollo che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo). Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio, progressivo di protocollo, data di protocollazione), mentre sono oscurati i dati relativi al profilo del protocollo (ad esempio, classificazione).

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

[63] Art. 24, comma 7, D. Lgs. 241/1990; Art. 59 e 60, D. Lgs. 196/2003.

Firmato digitalmente da Frighetto Iole Antonella

6.2.2. ACCESSO CIVICO GENERALIZZATO (FOIA)

Il diritto all'accesso civico generalizzato (FOIA) riguarda la possibilità di accedere a dati, documenti e informazioni detenuti dalle Pubbliche Amministrazioni ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria previsti dal D.Lgs. 33/2013[64].

Le istanze possono essere presentate da chiunque, a prescindere da particolari requisiti di qualificazione, e senza necessità di motivazione.

L'accesso civico generalizzato è volto a:

- assicurare a chiunque l'accesso indipendentemente dalla titolarità di situazioni giuridiche soggettive;
- promuovere la partecipazione al dibattito pubblico;
- favorire forme diffuse di controllo sul perseguimento delle finalità istituzionali e sull'utilizzo delle risorse pubbliche.

Le Istituzioni scolastiche, al fine di esaminare le istanze, dovrebbero adottare anche adeguate soluzioni organizzative, quali, ad esempio, *"la concentrazione della competenza a decidere sulle richieste di accesso in un unico ufficio (dotato di risorse professionali adeguate, che si specializzano nel tempo, accumulando know how ed esperienza), che, ai fini istruttori, dialoga con gli uffici che detengono i dati richiesti*", come indicato nella Deliberazione ANAC 1309/2016[65].

Fatto salvo quanto sopra, le scuole destinatarie dell'istanza, devono emettere un provvedimento espresso e motivato nei successivi trenta giorni.

Si rappresenta che l'accesso civico generalizzato è limitato qualora sia pregiudicato un interesse pubblico, ovvero:

- la sicurezza pubblica e l'ordine pubblico;
- la sicurezza nazionale;
- la difesa e le questioni militari;
- le relazioni internazionali;
- la politica e la stabilità finanziaria ed economica dello Stato;
- la conduzione di indagini sui reati e il loro perseguimento;
- il regolare svolgimento di attività ispettive.

L'Istituzione scolastica deve, altresì, effettuare un'attività valutativa con la tecnica del bilanciamento, caso per caso, tra l'interesse pubblico alla *disclosure* generalizzata e la tutela di

---

[64] L'accesso civico generalizzato è previsto dall'art. 5, comma 2, del D.Lgs. 33/2013 e si differenzia dall'accesso civico semplice di cui al comma 1 del medesimo articolo, il quale stabilisce che "*L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione*". Come precedentemente evidenziato, l'istanza di accesso civico, qualora abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013, è presentata al Responsabile per la prevenzione della corruzione e della trasparenza.

[65] La Deliberazione ANAC n. 1309 del 28 dicembre 2016, recante "*Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 c. 2 del D.Lgs. 33/2013*" è stata adottata ai sensi dell'art. 5-*bis*, comma 6, del D.Lgs. 33/2013 il quale stabilisce che "*Ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità nazionale anticorruzione, d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni operative*".

Firmato digitalmente da Frighetto Iole Antonella

interessi considerati validi dall'ordinamento. Il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

- protezione dei dati personali;
- libertà e segretezza della corrispondenza;
- interessi economici e commerciali, inclusi la proprietà intellettuale, il diritto d'autore e i segreti commerciali[66].

Sulle richieste di riesame presentate dai richiedenti ai quali sia stato negato totalmente o parzialmente l'accesso o che non abbiano avuto risposta entro il termine stabilito, il Responsabile per la prevenzione della corruzione e della trasparenza decide con provvedimento motivato, entro il termine di venti giorni.

Qualora l'accesso sia stato negato o differito per esigenze di tutela della protezione dei dati personali, il Responsabile della prevenzione della corruzione e della trasparenza, fatto salvo il confronto con il RPD, deve provvedere, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta.

Il termine per l'adozione del provvedimento da parte del RPCT è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni[67].

Nei casi di risposta negativa o parzialmente negativa sopra elencati, l'Istituzione scolastica è tenuta, ad ogni modo, a una congrua e completa motivazione.

Specifiche indicazioni e raccomandazioni operative sul FOIA sono contenute nella Circolare del Ministro per la Semplificazione e la Pubblica Amministrazione n. 2/2017 avente ad oggetto "*Attuazione delle norme sull'accesso civico generalizzato (c.d. FOIA)*", in particolare:

- uffici competenti;
- tempi di decisione;
- controinteressati;
- rifiuti non consentiti;
- dialogo con i richiedenti;
- Registro degli accessi.

Il 28 giugno 2019 il Ministero della Pubblica Amministrazione ha adottato, inoltre, la circolare n. 1/2019 allo scopo di fornire alle Pubbliche Amministrazioni "*indirizzi e chiarimenti*" ulteriori rispetto alle "*raccomandazioni operative*" di cui alla circolare n. 2/2017 ed alle Linee Guida dell'ANAC adottate d'intesa con il Garante per la protezione dei dati personali nel 2016. I profili trattati riguardano:

- criteri applicativi di carattere generale;
- regime dei costi;
- notifica ai controinteressati;
- partecipazione dei controinteressati alla fase di riesame;
- termine per proporre l'istanza di riesame;
- strumenti tecnologici di supporto.

---

[66] Si vedano, sul punto, l'art. 5-*bis* del D.Lgs. 33/2013 e la Deliberazione ANAC 1309/2016.
[67] Art. 5, comma 7, del D.Lgs. 33/2013.

Firmato digitalmente da Frighetto Iole Antonella

6.2.3. Registro degli accessi

Il registro delle richieste di accesso presentate per tutte le tipologie di accesso è istituito presso l'Istituzione scolastica, in conformità a quanto stabilito dai già citati documenti, ovvero, la Deliberazione ANAC n. 1309/2016, nonché dalla Circolare del Ministro per la Pubblica Amministrazione n. 2/2017, e dalla successiva Circolare del Ministro per la Pubblica Amministrazione n. 1/2019.

Il registro è costituito attraverso la raccolta organizzata delle richieste con l'indicazione dell'oggetto, della data e del relativo esito (con data della decisione), il quale sarà pubblicato sul sito istituzionale dell'Istituzione scolastica con cadenza trimestrale. L'implementazione del registro avviene mediante l'utilizzo del sistema di protocollo informatico e dei flussi documentali di cui è dotata l'Istituzione scolastica ai sensi del D.P.R. n. 445 del 2000, del CAD e delle relative regole tecniche.

7. Allegati

- 7.1 Articolazione della AOO e delle eventuali UOR
- 7.2 Titolario unico di classificazione
- 7.3 Piano di organizzazione delle aggregazioni documentali
- 7.4 Elenco dei documenti soggetti a registrazione particolare per tutte le amministrazioni
- 7.5 Trattamento delle registrazioni particolari: registri e modalità di gestione
- 7.6 Politiche di sicurezza

Il Dirigente Scolastico

Dott.ssa Iole Antonella Frighetto

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

Ministero dell'Istruzione,

"Liceo Scientifico Da Vinci"

Allegati al

Manuale di Gestione

Del Protocollo Informatico

Firmato digitalmente da Frighetto Iole Antonella

7.1 Articolazioni delle AOO e delle UOR

Sezione AOO

Denominazione dell'Amministrazione	**"Liceo Scientifico Da Vinci"**
Codice identificativo assegnato all'Amministrazione *(Codice univoco AOO)*	
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	ARZIGNANO (VI)
Nominativo del Responsabile del Servizio di Protocollo informatico, gestione documentale e archivistica	
Casella di posta elettronica istituzionale dell'AOO	
Data di istituzione della AOO	

Sezione UOR

Denominazione dell'UOR	**Ufficio per la transizione al digitale**
Codice univoco assegnato all'UOR	*(Riportare il codice univoco dell'UOR Ufficio per la transizione al digitale indicato su IndicePA)*
Indirizzo completo della sede principale dell'UOR a cui indirizzare l'eventuale corrispondenza convenzionale	Viale Trastevere 76/a - 00153 Roma (RM)
Codice fiscale FSE	*(non compilare)*
Codice fiscale NSO	*(non compilare)*
Nominativo del Responsabile	Ministero dell'istruzione RTD

Casella di posta dell'UOR	rtd@istruzione.it

Da compilare secondo necessità per ogni ulteriore UOR (eventuale Ufficio Fatturazione o altre UOR indicate all'interno di IndicePA)

Denominazione dell'UOR	*(Riportare la denominazione dell'UOR)*
Codice univoco assegnato all'UOR	*(Riportare il codice univoco dell'UOR indicato su IndicePA)*
Indirizzo completo della sede principale dell'UOR a cui indirizzare l'eventuale corrispondenza convenzionale	ARZIGNANO (VI)
Codice fiscale FSE	*(non compilare)*
Codice fiscale NSO	*(non compilare)*
Nominativo del Responsabile	*(Riportare il nominativo del Responsabile dell'UOR indicato su IndicePA)*
Casella di posta dell'UOR	

7.2 Titolario unico di classificazione

I AMMINISTRAZIONE

I.1 Normativa e disposizioni attuative

I.2 Organigramma e funzionigramma

I.3 Statistica e sicurezza di dati e informazioni

I.4 Archivio, accesso, privacy, trasparenza e relazioni con il pubblico

I.5 Registri e repertori di carattere generale

I.6 Audit, qualità, carta dei servizi, valutazione e autovalutazione

I.7 Elezioni e nomine

I.8 Eventi, cerimoniale, patrocini, concorsi, editoria e stampa

II ORGANI E ORGANISMI

II.1 Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione

II.2 Consiglio di classe e di interclasse

II.3 Collegio dei docenti

II.4 Giunta esecutiva

II.5 Dirigente scolastico DS

II.6 Direttore dei servizi generali e amministrativi DSGA

II.7 Comitato di valutazione del servizio dei docenti

II.8 Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia

II.9 Reti scolastiche

II.10 Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)

II.11 Commissioni e gruppi di lavoro

III ATTIVITÀ GIURIDICO-LEGALE

III.1 Contenzioso

III.2 Violazioni amministrative e reati

III.3 Responsabilità civile, penale e amm.va

III.4 Pareri e consulenze

IV DIDATTICA

IV.1 Piano triennale dell'offerta formativa PTOF

IV.2 Attività extracurricolari

IV.3 Registro di classe, dei docenti e dei profili

IV.4 Libri di testo

IV.5 Progetti e materiali didattici

IV.6 Viaggi di istruzione, scambi, stage e tirocini

IV.7 Biblioteca, emeroteca, videoteca e sussidi

IV.8 Salute e prevenzione

IV.9 Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo

IV.10 Elaborati e prospetti scrutini

V STUDENTI E DIPLOMATI

V.1 Orientamento e placement

V.2 Ammissioni e iscrizioni

V.3 Anagrafe studenti e formazione delle classi

V.4 Cursus studiorum

V.5 Procedimenti disciplinari

V.6 Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)

V.7 Tutela della salute e farmaci

V.8 Esoneri

V.9 Prescuola e attività parascolastiche

V.10 Disagio e diverse abilità – DSA

VI FINANZA E PATRIMONIO

VI.1 Entrate e finanziamenti del progetto

VI.2 Uscite e piani di spesa

VI.3 Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili

VI.4 Imposte, tasse, ritenute previdenziali e assistenziali, denunce

VI.5 Assicurazioni

VI.6 Utilizzo beni terzi, comodato

VI.7 Inventario e rendiconto patrimoniale

VI.8 Infrastrutture e logistica (plessi, succursali)

VI.9 DVR e sicurezza

VI.10 Beni mobili e servizi

VI.11 Sistemi informatici, telematici e fonia

VII PERSONALE

VII.1 Organici, lavoratori socialmente utili, graduatorie

VII.2 Carriera

VII.3 Trattamento giuridico-economico

VII.4 Assenze

VII.5 Formazione, aggiornamento e sviluppo professionale

VII.6 Obiettivi, incarichi, valutazione e disciplina

VII.7 Sorveglianza sanitaria

VII.8 Collaboratori esterni

7.3 Piano di organizzazione delle aggregazioni documentali

MASSIMARIO DI CONSERVAZIONE E SCARTO PER LE ISTITUZIONI SCOLASTICHE

STRUTTURA DEL MASSIMARIO

Al fine di garantire l'integrazione del massimario con il sistema di classificazione, la struttura del massimario si articola su tre livelli: il primo e il secondo livello corrispondono rispettivamente al titolo (I livello) e alla classe (II livello) del titolario di classificazione. Il terzo livello definisce le tipologie documentarie associate a ciascuna classe; per ciascuna tipologia documentaria sono fornite indicazioni in merito ai tempi di conservazione.

Ciò premesso, al fine di agevolare la consultazione del documento, si riporta di seguito la struttura del massimario.

I. AMMINISTRAZIONE

I.1 Normativa e disposizioni attuative
I.2 Organigramma e funzionigramma
I.3 Statistica e sicurezza di dati e informazioni
I.4 Archivio, accesso, privacy, trasparenza e relazioni con il pubblico
I.5 Registri e repertori di carattere generale
I.6 Audit, qualità, carta dei servizi, valutazione e autovalutazione
I.7 Elezioni e nomine
I.8 Eventi, cerimoniale, patrocini, concorsi, editoria e stampa

II. ORGANI E ORGANISMI

II.1 Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione
II.2 Consiglio di classe e di interclasse
II.3 Collegio dei docenti
II.4 Giunta esecutiva
II.5 Dirigente scolastico DS
II.6 Direttore dei servizi generali e amministrativi DSGA
II.7 Comitato di valutazione del servizio dei docenti
II.8 Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia
II.9 Reti scolastiche
II.10 Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)
II.11 Commissioni e gruppi di lavoro

III. ATTIVITÀ GIURIDICO-LEGALE

III.1 Contenzioso
III.2 Violazioni amministrative e reati
III.3 Responsabilità civile, penale e amm.va
III.4 Pareri e consulenze

IV. DIDATTICA

IV.1 Piano triennale dell'offerta formativa PTOF
IV.2 Attività extracurricolari
IV.3 Registro di classe, dei docenti e dei profili
IV.4 Libri di testo
IV.5 Progetti e materiali didattici
IV.6 Viaggi di istruzione, scambi, stage e tirocini
IV.7 Biblioteca, emeroteca, videoteca e sussidi
IV.8 Salute e prevenzione

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

IV.9 Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo
IV.10 Elaborati e prospetti scrutini

V. STUDENTI E DIPLOMATI

V.1 Orientamento e placement
V.2 Ammissioni e iscrizioni
V.3 Anagrafe studenti e formazione delle classi
V.4 Cursus studiorum
V.5 Procedimenti disciplinari
V.6 Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)
V.7 Tutela della salute e farmaci
V.8 Esoneri
V.9 Prescuola e attività parascolastiche
V.10 Disagio e diverse abilità – DSA

VI. FINANZA E PATRIMONIO

VI.1 Entrate e finanziamenti del progetto
VI.2 Uscite e piani di spesa
VI.3 Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili
VI.4 Imposte, tasse, ritenute previdenziali e assistenziali, denunce
VI.5 Assicurazioni
VI.6 Utilizzo beni terzi, comodato
VI.7 Inventario e rendiconto patrimoniale
VI.8 Infrastrutture e logistica (plessi, succursali)
VI.9 DVR e sicurezza
VI.10 Beni mobili e servizi
VI.11 Sistemi informatici, telematici e fonia

VII. PERSONALE

VII.1 Organici, lavoratori socialmente utili, graduatorie
VII.2 Carriera
VII.3 Trattamento giuridico-economico
VII.4 Assenze
VII.5 Formazione, aggiornamento e sviluppo professionale
VII.6 Obiettivi, incarichi, valutazione e disciplina
VII.7 Sorveglianza sanitaria
VII.8 Collaboratori esterni

Firmato digitalmente da Frighetto Iole Antonella

I LIVELLO: Amministrazione

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.1	**Normativa e disposizioni attuative**	I.1.1	Leggi, regolamenti e tutta la documentazione relativa a: - istituzione della scuola - intitolazione - eventuali accorpamenti e trasformazioni (ad es. in istituto comprensivo)	ILLIMITATI
		I.1.2	Norme e regolamenti interni (regolamento dell'istituto, carta dei servizi, regolamenti della biblioteca, dei laboratori e direttive varie ecc.)	ILLIMITATI
		I.1.3	Norme e disposizioni Economato	ILLIMITATI
		I.1.4	Norme e disposizioni relative al personale e CCNL	50 anni dall'entrata in vigore
		I.1.5	Circolari e ordinanze interne esplicative e direttive	ILLIMITATI di almeno 1 esemplare per circolare/ordinanza
		I.1.6	Norme e disposizioni relative all'archivio	ILLIMITATI
		I.1.7	Norme e disposizioni relative a pensione e trattamento di quiescenza	Scartabile dopo 10 anni dalla decadenza
		I.1.8	Regolamenti delle biblioteche dell'Istituto (dei docenti, degli alunni, ecc)	ILLIMITATI
I.2	**Organigramma e funzionigramma**	I.2.1	Documentazione relativa a organico dell'autonomia, organico docenti, organico ATA	ILLIMITATI
I.3	**Statistica e sicurezza di dati e informazioni**	I.3.1	Documento programmatico di sicurezza dati (DPS)	ILLIMITATI
		I.3.2	Inchieste, indagini (ambientali, socio-economiche, sanitarie, ecc.)	ILLIMITATI
		I.3.3	Statistiche	ILLIMITATI
I.4	**Archivio, accesso, privacy, trasparenza e relazioni con il pubblico**	I.4.1	Documenti relativi alla privacy e alla protezione dei dati	ILLIMITATI
		I.4.2	Titolari di classificazione d'archivio (compresi quelli non più in uso)	ILLIMITATI
		I.4.3	Scarto di atti d'archivio (procedure, elenchi, autorizzazioni e verbali di distruzione…)	ILLIMITATI
		I.4.4	Registri di protocollo (generali e riservati)	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.4	**Archivio, accesso, privacy, trasparenza e relazioni con il pubblico**	I.4.5	Repertori dei fascicoli d'archivio	ILLIMITATI
		I.4.6	Rubriche alfabetiche del protocollo	ILLIMITATI
		I.4.7	Registro della posta in partenza e/o documentazione attestante la spedizione o la ricezione (anche a mano o mediante affissione in bacheca)	10 anni dalla data dell'ultima registrazione (salvo contenziosi in corso)
		I.4.8	Richiesta di accesso ai documenti	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle richieste (salvo contenziosi in corso)
		I.4.9	Richieste di copie di atti e relativo rilascio	Scartabili dopo 1 anno, conservando illimitatamente eventuali registri delle copie rilasciate
		I.4.10	Richieste di certificati e loro trasmissione	Scartabili dopo 6 anni

Firmato digitalmente da Frighetto Iole Antonella

		I.4.11	Bollettario di richiesta degli stampati	Scartabile dopo 6 anni
		I.4.12	Richieste di consultazione dell'archivio della scuola per finalità storico-culturali	Scartabili dopo 6 anni, conservando illimitatamente il registro delle consultazioni
I.5	**Registri e repertori di carattere generale**	I.5.1	Registro verbali riunioni per contrattazione d'istituto	ILLIMITATI
		I.5.2	Registri dei verbali del Consiglio o Staff di Presidenza	ILLIMITATI
		I.5.3	Registri dei verbali degli Organi collegiali (Consiglio di circolo o di istituto, Giunta esecutiva, Collegio docenti, Consigli di classe o di interclasse) e degli eventuali gruppi di lavoro derivati (es. dipartimenti, commissioni, ambiti disciplinari ecc)	ILLIMITATI
		I.5.4	Registro delle deliberazioni	ILLIMITATI
		I.5.5	Registri dei contratti per fornitura di materiali, espletamento di servizi, assunzione personale	ILLIMITATI
		I.5.6	Registro cronologico dei contratti	ILLIMITATI
		I.5.7	Registri dei verbali della cassa scolastica	ILLIMITATI
		I.5.8	Registri dei materiali di facile consumo	Scartabili dopo 10 anni

II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.5	**Registri e repertori di carattere generale**	I.5.9	Registro delle tasse e dei contributi scolastici (iscrizione, diploma…)	Scartabile dopo 10 anni dall'ultima registrazione, conservando a campione una annata ogni dieci
		I.5.10	Registro dei verbali dei Revisori dei conti	ILLIMITATI
		I.5.11	Inventari patrimoniali (registri inventariali) dei beni mobili; registri di entrata della biblioteca; registri di entrata dei sussidi multimediali; inventari e repertori dell'archivio	ILLIMITATI
		I.5.12	Registro di magazzino	Scartabile dopo 6 anni
		I.5.13	Registro licenze software	ILLIMITATI
		I.5.14	Registro delle tessere di riconoscimento (Mod. AT)	ILLIMITATI
		I.5.15	Registri delle autorizzazioni ad impartire lezioni private	Scartabili dopo 6 anni dall'ultima registrazione
		I.5.16	Registri dello stato personale	ILLIMITATI
		I.5.17	Registro degli stipendi ed altri assegni	ILLIMITATI
		I.5.18	Registri degli infortuni	ILLIMITATI
		I.5.19	Registri dei certificati di servizio rilasciati dalla scuola	ILLIMITATI
		I.5.20	Registri assenze	Scartabili dopo 50 anni
		I.5.21	Registri di immatricolazione e/o di iscrizione degli alunni	ILLIMITATI
		I.5.22	Registri generali dei voti, delle valutazioni	ILLIMITATI

		I.5.23	Registri dei certificati di studio rilasciati dalla scuola	ILLIMITATI
		I.5.24	Registri e verbali del debito formativo	Scartabili dopo 10 anni, conservando illimitatamente un anno a campione ogni 5
		I.5.25	Registro riunioni per materia	ILLIMITATI
II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.5	**Registri e repertori di carattere generale**	I.5.26	Registro riunioni per dipartimento	ILLIMITATI
		I.5.27	Registri dei verbali degli scrutini	ILLIMITATI
		I.5.28	Registri dei verbali degli esami e delle relative prove	ILLIMITATI
		I.5.29	Registri di carico e scarico dei diplomi	ILLIMITATI
		I.5.30	Registri di consegna dei diplomi	ILLIMITATI
I.6	**Audit, qualità, carta dei servizi, valutazione e autovalutazione**	I.6.1	Certificazioni di qualità e accreditamenti (es. ministeriali e regionali, ecc.)	ILLIMITATI
		I.6.2	Verbali di ispezione	ILLIMITATI
		I.6.3	Relazioni finali di istituto	ILLIMITATI
		I.6.4	Questionari e monitoraggio	Scartabili dopo un anno, conservando illimitatamente una copia in bianco del questionario e i suoi risultati sintetici
		I.6.5	Valutazioni, rilevazioni dati, e relazioni sull'attività della scuola, redatte sia da personale interno sia da esterni (INVALSI, OCSE- PISA, ecc.)	ILLIMITATI
I.7	**Elezioni e nomine**	I.7.1	Verbali delle Commissioni Elettorali. Atti di nomina degli Organi collegiali a livello di circolo e di istituto	ILLIMITATI
		I.7.2	Atti delle elezioni degli Organi collegiali: - verbale di consegna di materiale elettorale - liste candidati - elenchi elettori - certificati elettorali - scheda votazioni - prospetti per il calcolo dei voti - tabelle scrutinio	Scartabili dopo 6 anni dalle elezioni conservando 1 campione di scheda non utilizzata per ciascuna elezione e per ciascuna categoria di elettori
		I.7.3	Atti di nomina di commissioni, comitati, e gruppi di lavoro	ILLIMITATI
I.8	**Eventi, cerimoniale, patrocini, concorsi, editoria e stampa**	I.8.1	Documentazione relativa a cerimonie, inaugurazioni e relazioni esterne	Scartabili dopo 10 anni
		I.8.2	Giornalini di classe o d'istituto	ILLIMITATI di almeno un esemplare
II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
I.8	**Eventi, cerimoniale, patrocini, concorsi, editoria e stampa**	I.8.3	Annuari, rassegna stampa e pubblicazioni varie della scuola	ILLIMITATI di almeno un esemplare degli annuari e delle pubblicazioni e della rassegna stampa
		I.8.4	Locandine e manifesti di qualsiasi tipo pubblicati o stampati dalla o per conto della scuola	Scartabili dopo 10 anni

I LIVELLO: Organi e organismi

Firmato digitalmente da Frighetto Iole Antonella

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
II.1	**Consiglio di istituto, Consiglio di circolo e Consiglio di Amministrazione**	II.1.1	Verbali Consiglio di Istituto e Consiglio di circolo	ILLIMITATI
		II.1.2	Verbali del Consiglio di Amministrazione	ILLIMITATI
		II.1.3	Convocazioni riunioni Consiglio di istituto e Consiglio di circolo	Scartabili dopo 6 anni
II.2	**Consiglio di classe e di interclasse**	II.2.1	Verbali Consiglio di classe e di interclasse	ILLIMITATI
		II.2.2	Convocazioni riunioni Consiglio di classe e di interclasse	Scartabili dopo 6 anni
II.3	**Collegio dei docenti**	II.3.1	Verbali Collegio dei docenti	ILLIMITATI
		II.3.2	Convocazioni riunioni Collegio dei docenti	Scartabili dopo 6 anni
II.4	**Giunta esecutiva**	II.4.1	Verbali Giunta esecutiva	ILLIMITATI
		II.4.2	Convocazioni riunioni Giunta esecutiva	Scartabili dopo 6 anni
II.5	**Dirigente scolastico DS**	II.5.1	Determinazioni dirigenziali (raccolte in serie cronologiche)	ILLIMITATI
		II.5.2	Piano delle attività dei docenti	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
II. 6	**Direttore dei servizi generali e amministrativi DSGA**	II.6.1	Ordini di servizio generali	ILLIMITATI
		II.6.2	Piano delle attività del personale ATA	ILLIMITATI
II. 7	**Comitato di valutazione del servizio dei docenti**	II.7.1	Verbali di valutazione dei docenti	ILLIMITATI
		II.7.2	Convocazione riunioni Comitato di valutazione	Scartabili dopo 5 anni
II. 8	**Comitato dei genitori, Comitato studentesco e rapporti scuola-famiglia**	II.8.1	Comunicazioni da parte di Comitato studentesco, Comitato dei genitori e famiglie	Scartabili dopo 5 anni
		II.8.2	Verbali di Comitato studentesco e Comitato dei genitori	ILLIMITATI
		II.8.3	Convocazione riunioni Comitato studentesco e Comitato dei genitori	Scartabili dopo 5 anni
II. 9	**Reti scolastiche**	II.9.1	Convenzioni e accordi di rete (con scuole, con enti ecc.)	ILLIMITATI
II. 10	**Rapporti sindacali, contrattazione e Rappresentanza sindacale unitaria (RSU)**	II.10. 1	Contrattazione d'istituto	ILLIMITATI
		II.10. 2	- Rapporti con organizzazioni sindacali e rappresentanze interne - Scioperi	ILLIMITATI
II. 11	**Commissioni e gruppi di lavoro**	II.11. 1	Verbali, documenti istruttori e deliberativi di Commissioni e gruppi di lavoro	ILLIMITATI
		II.11. 2	Convocazione riunioni delle Commissioni e gruppi di lavoro	Scartabili dopo 5 anni

I LIVELLO: Attività giuridico-legale

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
III.1	**Contenzioso**	III.1.1	Documentazione prodotta e acquisita nel corso di transazioni, conciliazioni e ricorsi amministrativi e giurisdizionali	ILLIMITATI
		III.1.2	Azioni legali collettive del personale	ILLIMITATI
II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
III.2	**Violazioni amministrative e reati**	III.2.1	Documentazione relativa a violazioni amministrative e reati (denunce alle forze dell'ordine, sanzioni amministrative, ecc.)	ILLIMITATI
III.3	**Responsabilità civile, penale e amm.va**	III.3.1	Recupero retribuzione dipendenti assenti dal lavoro per responsabilità di terzi	Scartabile dopo 50 anni
III.4	**Pareri e consulenze**	III.4.1	Relazioni su collaborazioni con (o consulenze da parte di): - istituzioni socio-assistenziali - enti locali - cooperative ed associazioni - Tribunale dei minori - servizio sanitario nazionale	ILLIMITATI
		III.4.2	Pareri legali	ILLIMITATI

I LIVELLO: Didattica

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
IV.1	**Piano Triennale dell'Offerta Formativa PTOF**	IV.1.1	Piano Triennale dell'Offerta Formativa (PTOF)	ILLIMITATI
IV.2	**Attività extracurricolari**	IV.2.1	Attività formative (teatro, musica, interventi di recupero, inserimento alunni stranieri, patentino ecc.)	ILLIMITATI
		IV.2.2	Progetti operativi nazionali (PON); Progetti operativi regionali (POR);	ILLIMITATI
		IV.2.3	Documentazione per programmazione ed attuazione di attività scolastiche anche esterne (manifestazioni teatrali, ecc.)	Scartabile dopo 6 anni, conservando illimitatamente a campione un'annata ogni 10
IV.3	**Registro di classe, dei docenti e dei profili**	IV.3.1	Recupero orario: relazioni, dichiarazioni e autocertificazioni	Scartabili dopo 10 anni
		IV.3.2	Orari delle lezioni	ILLIMITATI di un esemplare dell'orario di ciascuna classe di tutte le sezioni, scartando dopo un anno eventuali copie d'uso e dopo 6 anni gli atti relativi alla definizione dell'orario
II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
		IV.3.3	Registri dei profili degli alunni redatti dai Consigli di classe	ILLIMITATI

Firmato digitalmente da Frighetto Iole Antonella

IV. 3	**Registro di classe, dei docenti e dei profili**	IV.3.4	Registri di classe	ILLIMITATI
		IV.3.5	Registri personali dei docenti	ILLIMITATI fino all'anno scolastico 1969/70. Successivamente scartabili dopo 10 anni, conservando illimitatamente un anno ogni 5
		IV.3.6	Registri delle assenze degli alunni (e relativa documentazione)	Scartabili dopo 6 anni
IV. 4	**Libri di testo**	IV.4.1	Verbali e relazioni riguardanti l'adozione dei libri di testo	ILLIMITATI
IV. 5	**Progetti e materiali didattici**	IV.5.1	Piani di lavoro, Programmi, Relazioni finali di classe	ILLIMITATI
		IV.5.2	Piano Educativo Individualizzato (PEI)	ILLIMITATI nel fascicolo personale dell'alunno
		IV.5.3	Programmi d'esame	ILLIMITATI
		IV.5.4	Documenti prodotti da docenti e studenti in preparazione e nel corso di attività didattiche (dispense, percorsi, sussidi, sperimentazioni multidisciplinari, testi teatrali, sceneggiature cinematografiche ecc.)	ILLIMITATI di almeno un esemplare
		IV.5.5	Progetti curricolari	ILLIMITATI
IV. 6	**Viaggi di istruzione, scambi, stage e tirocini**	IV.6.1	Pratiche per assistenza e soggiorni climatici /colonie	ILLIMITATI
		IV.6.2	Borse di studio / stage: bandi, studi e relazioni	ILLIMITATI
		IV.6.3	Documentazione per programmazione ed attuazione di attività scolastiche anche esterne (gite, visite di studio ecc.)	Scartabile dopo 6 anni, conservando illimitatamente a campione un'annata ogni 10
		IV.6.4	Documentazione relativa ai PCTO (Percorsi per le Competenze Trasversali e l'Orientamento)	ILLIMITATI
IV. 7	**Biblioteca, emeroteca, videoteca e sussidi**	IV.7.1	Contributi per biblioteca scolastica (documentazione relativa)	Scartabili dopo 6 anni, conservando illimitatamente il registro cronologico di entrata (vedi I.5.11)
		IV.7.2	Cataloghi e regolamenti delle biblioteche dell'Istituto (dei docenti, degli alunni, ecc)	ILLIMITATI
IV. 8	**Salute e prevenzione**	IV.8.1	Educazione alla salute: progetti, interventi e convenzioni	ILLIMITATI

II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
IV. 9	**Attività sportivo-ricreative e rapporti con il Centro Scolastico Sportivo**	IV.9.1	Autorizzazioni all'uso di locali scolastici e impianti sportivi	Scartabili dopo 6 anni, conservando eventuali atti riassuntivi
		IV.9.2	Progetti formativi relativi a sport	ILLIMITATI
		IV.9.3	Registri attività del Gruppo sportivo	Scartabili dopo 10 anni
IV. 10	**Elaborati e prospetti scrutini**	IV.10.1	Elaborati delle prove scritte, grafiche e pratiche degli alunni (esclusi quelli prodotti per l'esame di Stato)	Scartabili dopo un anno, conservando illimitatamente a campione una annata ogni 10
		IV.10.2	Elaborati delle prove scritte, grafiche per gli esami di Stato	ILLIMITATI nel plico dell'esame
		IV.10.3	Elaborati delle prove pratiche per gli esami di Stato	Scartabili dopo un anno conservando nel plico dell'esame le fotografie dei manufatti

		IV.10.4	Elaborati delle prove Invalsi	Scartabili dopo un anno, conservando illimitatamente a campione una annata ogni 10
		IV.10.5	Prospetti scrutini trimestrali o quadrimestrali	ILLIMITATI
		IV.10.6	Prospetti scrutinio finale	ILLIMITATI

I LIVELLO: Studenti e diplomati

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V. 1	**Orientamento e placement**	V.1.1	Progetti formativi relativi a orientamento e placement	ILLIMITATI
V. 2	**Ammissioni e iscrizioni**	V.2.1	Elenchi alunni per iscrizioni	Scartabili dopo 10 anni
		V.2.2	Domande e documenti prodotti da alunni e candidati per l'iscrizione ai vari tipi di scuola e per l'ammissione agli esami	Scartabili dopo 6 anni dalla fine dell'appartenenza all'Istituto o dall'iscrizione all'esame
V. 3	**Anagrafe studenti e formazione delle classi**	V.3.1	Certificati di nascita	Scartabili dopo 6 anni dalla cessazione dell'appartenenza all'Istituto o dall'iscrizione agli esami, con l'eccezione dei documenti degli allievi stranieri
II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V. 3	**Anagrafe studenti e formazione delle classi**	V.3.2	Documentazione relativa alla formazione delle classi	Scartabili dopo 10 anni
V. 4	***Cursus studiorum***	V.4.1	Relazioni inerenti le ripetenze degli alunni	ILLIMITATI nei rispettivi fascicoli personali
		V.4.2	Fascicoli personali alunni	ILLIMITATI
		V.4.3	Pagelle scolastiche Schede di valutazione Schede alunni	ILLIMITATI
		V.4.4	Libretti scolastici e altra documentazione relativa agli studi dell'alunno (es. Portfolio)	ILLIMITATI
		V.4.5	Certificazioni delle competenze	ILLIMITATI
V. 5	**Procedimenti disciplinari**	V.5.1	Sanzioni disciplinari agli alunni	ILLIMITATI
V. 6	**Diritto allo studio e servizi agli studenti (trasporti, mensa, buoni libro, etc.)**	V.6.1	- Elenchi dei buoni libro concessi e documentazione di supporto - Cedole librarie	Scartabili dopo 6 anni, conservando illimitatamente l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali
		V.6.2	Mensa: richieste di iscrizione al servizio mensa ed elenchi presenze	Scartabili dopo 6 anni, conservando illimitatamente contratti, relazioni sull'attività, diete e menu seguiti
		V.6.3	Trasporto alunni: richieste di iscrizione al servizio ed attestazioni di pagamento	Scartabili dopo 6 anni
		V.6.4	Trasporto alunni: richieste per trasporto gratuito	Scartabili dopo 6 anni, conservando elenchi riassuntivi
		V.6.5	Certificazioni per richieste di abbonamenti ferroviari e diversi	Scartabili dopo 1 anno

		V.6.6	Documentazione riguardante assistenza scolastica e Patronato scolastico	ILLIMITATI
		V.6.7	Documentazione riguardante il diritto allo studio	ILLIMITATI
		V.6.8	Certificazioni per richieste ai fini della fruizione di assegni di studio	Scartabili dopo 10 anni
V. 7	**Tutela della salute e farmaci**	V.7.1	Certificati di vaccinazione	Scartabili dopo 6 anni dalla cessazione dell'appartenenza all'Istituto o dall'iscrizione agli esami, con l'eccezione dei documenti degli allievi stranieri
		V.7.2	Campagne di vaccinazione e disinfestazione, atti e documenti relativi alla loro effettuazione	Scartabili dopo 6 anni, conservando illimitatamente la documentazione e i registri riassuntivi

II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
V. 8	**Esoneri**	V.8.1	Documentazione relativa ad esoneri	ILLIMITATI nel fascicolo personale
V. 9	**Prescuola e attività parascolastiche**	V.9.1	Cooperative di alunni: atti costitutivi, documenti istruttori e deliberativi, corrispondenza	ILLIMITATI
		V.9.2	Convenzioni per attività formative e parascolastiche	ILLIMITATI
V. 10	**Disagio e diverse abilità – DSA**	V.10. 1	Schede individuali degli alunni (schedario)	ILLIMITATI

I LIVELLO: Finanza e patrimonio

II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI. 1	**Entrate e finanziamenti del progetto**	VI.1. 1	Partitario delle Entrate	ILLIMITATI
		VI.1. 2	Reversali con la relativa documentazione giustificativa (fatture, corrispondenza varia)	Scartabili dopo 10 anni (previa verifica della conservazione dei rispettivi giornali di cassa e partitari) conservando illimitatamente progetti, collaudi, perizie degli impianti e delle manutenzioni straordinarie delle attrezzature durevoli (macchinari tecnici, arredi di particolare interesse, ecc.)
VI. 2	**Uscite e piani di spesa**	VI.2. 1	Partitario delle Uscite	ILLIMITATI
		VI.2. 2	Mandati di pagamento con la relativa documentazione giustificativa (ordinativi di acquisto, buoni d'ordine, fatture, corrispondenza varia)	Scartabili dopo 10 anni (previa verifica della conservazione dei rispettivi giornali di cassa e partitari) conservando illimitatamente progetti, collaudi, perizie degli impianti e delle manutenzioni straordinarie delle attrezzature durevoli (macchinari tecnici, arredi di particolare interesse, ecc.)
		VI.2. 3	Registro delle spese su aperture di credito e rendiconto trimestrale	ILLIMITATI
		VI.2. 4	Liquidazioni consulenze	Scartabili dopo 50 anni

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.2	**Uscite e piani di spesa**	VI.2.5	Copie di delibere e/o di determine di liquidazione	Scartabili dopo 10 anni
VI.3	**Bilancio, tesoreria, cassa, istituti di credito e verifiche contabili**	VI.3.1	Bilanci o programmi annuali e conti consuntivi (in originale o nell'unica copia esistente)	ILLIMITATI
		VI.3.2	Giornale di cassa	ILLIMITATI
		VI.3.3	Convenzione di cassa con Istituto Cassiere	ILLIMITATI
		VI.3.4	Rapporti con Istituto Cassiere (corrispondenza)	Scartabili dopo 10 anni
		VI.3.5	Distinte di trasmissione al Tesoriere di reversali e mandati	Scartabili dopo 10 anni
		VI.3.6	Estratti conto bancari e postali	Scartabili dopo 10 anni
		VI.3.7	Registro delle operazioni di conto corrente postale	Scartabile dopo 10 anni
		VI.3.8	Bollettini di conto corrente postale, ricevute di versamento	Scartabili dopo 10 anni
		VI.3.9	Documentazione riguardante l'insediamento dei Revisori dei conti	ILLIMITATI
VI.4	**Imposte, tasse, ritenute previdenziali e assistenziali, denunce**	VI.4.1	Documentazione riguardante la tassa di raccolta rifiuti e Modello Unico Dichiarazione Ambientale (MUD)	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.4.2	Contributi – modello DM/10- INPS tabulati riepilogativi imponibili, regolarizzazioni contributive – personale, rapporti con INPS MODELLI EMENS (Denunce Retributive Mensili)	Scartabili dopo 50 anni
		VI.4.3	Modello 01/M (copia del datore di lavoro)	Archiviato nel fascicolo personale
		VI.4.4	D.M.A Denuncia mensile analitica	Scartabile dopo 50 anni
		VI.4.5	FONDO ESPERO	Scartabile dopo 50 anni
		VI.4.6	Modelli 101 – Modelli CUD – Modelli CU	Archiviati nel Fascicolo personale
		VI.4.7	Modello 770	Scartabile dopo 50 anni
		VI.4.8	Denunce annuali IRAP	Scartabili dopo 50 anni

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.4	**Imposte, tasse, ritenute previdenziali e assistenziali, denunce**	VI.4.9	Dichiarazione IVA	Scartabili dopo 10 anni
VI.5	**Assicurazioni**	VI.5.1	Documentazione relativa a polizze assicurative	ILLIMITATI
VI.6	**Utilizzo beni terzi, comodato**	VI.6.1	Immobili in uso (di proprietà di altri enti) - atti relativi a locazione e comodati degli immobili (sia di proprietà sia	ILLIMITATI

Firmato digitalmente da Frighetto Iole Antonella

			appartenenti ad altri enti) - progetti tecnici, planimetrie, verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L. 626/94)	
		VI.6.2	Immobili in uso (di proprietà di altri enti) - documentazione pervenuta in copia dagli enti proprietari, non compresa in quella descritta al punto A5/2	Scartabile dopo 10 anni
VI.7	**Inventario e rendiconto patrimoniale**	VI.7.1	Verbali di consegna ed elenchi di consistenza di archivi o altri beni inventariati	ILLIMITATI
		VI.7.2	Ricognizioni patrimoniali di scuole confluite	ILLIMITATI
		VI.7.3	Ricognizioni patrimoniali decennali	ILLIMITATI
		VI.7.4	Rivalutazioni patrimoniali quinquennali	ILLIMITATI
		VI.7.5	Verbali dei passaggi di consegna	ILLIMITATI
VI.8	**Infrastrutture e logistica (plessi, succursali)**	VI.8.1	Immobili di proprietà - progetti tecnici, contratti di costruzione, ristrutturazione e manutenzione - verbali e perizie di collaudo, autorizzazioni e certificazioni relative alla sicurezza e alla messa a norma dei locali e degli impianti (L.626/94) - atti relativi a donazioni, acquisti e vendite di immobili di proprietà	ILLIMITATI
VI.9	**DVR e sicurezza**	VI.9.1	Documento valutazione dei rischi (L.626/94) e relativi allegati (es. piani di evacuazione, controlli periodici, nomine, ecc.)	ILLIMITATI
		VI.9.2	Protocolli di sicurezza	ILLIMITATI
VI.10	**Beni mobili e servizi**	VI.10.1	Contratti per fornitura di materiali e per espletamento di servizi	50 anni, conservando illimitatamente il relativo registro (vedi I.5.5)
		VI.10.2	Contratti di prestazione d'opera di varia natura	50 anni, conservando illimitatamente il relativo registro (vedi I.5.6)

II LIVELLO		**III LIVELLO**		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VI.10	**Beni mobili e servizi**	VI.10.3	Buoni d'acquisto, generi di refezione / di consumo	Scartabili dopo 6 anni
		VI.10.4	Abbonamenti e/o acquisti a giornali, riviste e pubblicazioni: corrispondenza relativa	Scartabile dopo 6 anni, conservando illimitatamente gli elenchi dei periodici in abbonamento e delle pubblicazioni acquistate
		VI.10.5	Acquisto di attrezzature, materiale, interventi di manutenzione: corrispondenza relativa	Scartabile dopo 10 anni
		VI.10.6	Acquisto di materiale di consumo: corrispondenza relativa	Scartabile dopo 6 anni, conservando i relativi Registri di materiale facile consumo (vedi I.5.8)
		VI.10.7	Verbali di collaudo di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso
		VI.10.8	Certificati di garanzia di apparecchiature ed attrezzature	Scartabili dopo la dismissione del bene, salvo contenzioso in corso
		VI.10.9	Dotazioni strumentali: richieste di intervento	Scartabili dopo 6 anni

		VI.10.10	“Libretto di macchina” degli autoveicoli in dotazione presso l’istituto	Scartabile dopo 6 anni
		VI.10.11	Documentazione riguardante le utenze (elettricità, ecc.)	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.10.12	Impianti ed attrezzature durevoli: disegni tecnici, progetti	ILLIMITATA
		VI.10.13	Buoni di carico	Scartabili dopo la dismissione del bene
		VI.10.14	Buoni di scarico	Scartabili dopo 10 anni dalla dismissione del bene o in sede di rinnovo degli inventari
VI.11	**Sistemi informatici, telematici e fonia**	VI.11.1	Documentazione riguardante le utenze di fonia	Scartabile dopo 10 anni salvo contenziosi in atto
		VI.11.2	Registri delle licenze software	ILLIMITATI

I LIVELLO: Personale

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.1	**Organici, lavoratori socialmente utili, graduatorie**	VII.1.1	Contratti assunzione personale	50 anni, conservando illimitatamente il relativo registro (vedi I.5.5)
		VII.1.2	Graduatorie interne del personale in servizio	Scartabili dopo 10 anni
		VII.1.3	Graduatorie d'Istituto per supplenze personale docente e non docente	Scartabili dopo 10 anni dalla decadenza di validità
		VII.1.4	Domande di inserimento in graduatoria d'Istituto, con relativa documentazione, inerenti graduatorie non più in vigore	Scartabili dopo 10 anni dalla decadenza di validità della relativa graduatoria conservando a disposizione degli interessati eventuali titoli di studio allegati in originale
		VII.1.5	Domande di supplenza e relative graduatorie in calce	Scartabili dopo 1 anno
		VII.1.6	Decreti di esclusione dalla graduatoria e decreti di rettifica del punteggio	ILLIMITATI
VII.2	**Carriera**	VII.2.1	Fascicoli individuali del personale docente e non docente in servizio, in quiescenza, di ruolo e non di ruolo (ora T.I. e T.D.): - Decreti di nomina e contratti individuali - Presa di servizio - Decreti di trasferimento - Certificati di nascita e residenza del personale di ruolo - Stato di famiglia e relativa documentazione - Certificati di sana e robusta costituzione - Lettere di invito per l'assegnazione della sede - Ordini di servizio individuali - Decreti (per congedi maternità anticipata, ecc.) - Decreti congedi parentali - Decreti congedi straordinari - Permessi - Decreti aspettative - Titoli di studio, attestati di partecipazione a corsi di formazione, aggiornamento, ecc. - Posizioni previdenziali, stipendiali, tributarie - Riscatto periodi assicurativi - Cessione "quinto" dello stipendio - Modello 01/M - Modello 101 e CUD - Richieste accertamenti sanitari (visite fiscali e collegiali, referti)	ILLIMITATI

Firmato digitalmente da Frighetto Iole Antonella

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.2	**Carriera**	VII.2.2	- Accertamenti individuali infortuni e malattie professionali (documentazione sanitaria e tecnica) - Azioni legali del singolo dipendente - Pensione e trattamento di quiescenza - Certificati di servizio - Domande di trasferimento - Permessi di studio - Domande scatti anticipati - Autorizzazioni varie (lezioni private, esercizio a libere professioni, collaborazioni plurime, ecc.) - Rilascio della tessera ministeriale (ferroviaria) - Certificato del casellario giudiziale - Decreto di conferma in ruolo - Domande di ricostruzione di carriera	ILLIMITATI
		VII.2.3	Copie certificati di servizio	Scartabili dopo 5 anni
VII.3	**Trattamento giuridico-economico**	VII.3.1	Tabelle stipendi (nominative) Tabulati mensili riepilogativi retribuzioni	Scartabili dopo 50 anni
		VII.3.2	Compensi per lavoro straordinario, gruppi sportivi, funzioni strumentali e aggiuntive, incarichi specifici, funzioni miste, ore straordinarie per sostituzione colleghi assenti, ore di insegnamento aggiuntive, ore funzionali di non insegnamento, compensi da fondo istituto, o da fondi esterni, ecc.	Scartabili dopo 50 anni
		VII.3.3	Acconti e conguagli per il personale, riepiloghi	Scartabili dopo 50 anni
VII.4	**Assenze**	VII.4.1	Fogli di presenza e altri documenti per la rilevazione delle presenze	Scartabili dopo 10 anni, salvo contenzioso
		VII.4.2	Domande di ferie (congedo ordinario), permessi brevi	Scartabili dopo 6 anni
VII.5	**Formazione, aggiornamento e sviluppo professionale**	VII.5.1	Aggiornamento personale - programmi - relazioni finali - dispense - firme presenza - attestati	ILLIMITATI
VII.6	**Obiettivi, incarichi, valutazione e disciplina**	VII.6.1	Ruoli del personale: documenti istruttori e deliberativi, albi, elenchi, registri, ecc.	ILLIMITATI
		VII.6.2	Sanzioni disciplinari a docenti e personale ATA	ILLIMITATI
VII.7	**Sorveglianza sanitaria**	VII.7.1	Accertamenti sanitari e tecnici: documentazione relativa a malattie professionali, ecc.	ILLIMITATI

II LIVELLO		III LIVELLO		
ID	**Descrizione**	**ID**	**Tipologia documentaria**	**Tempi di conservazione**
VII.8	**Collaboratori esterni**	VII.8.1	Relazioni su collaborazioni con (o consulenze da parte di) esperti esterni	ILLIMITATI
		VII.8.2	Documentazione relativa agli esperti (CV, dichiarazioni altri incarichi, insussistenza conflitti di interesse, contratto d'incarico, ecc.)	ILLIMITATI

Firmato digitalmente da Frighetto Iole Antonella

7.4 – Elenco dei documenti soggetti a registrazione particolare per tutte le amministrazioni

• Documenti relativi a vicende di persone o a fatti privati o particolari;
• Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
• Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
• I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
• corrispondenza legata a vicende di persone o a fatti privati o particolari;
• le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241, dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

7.5 – Trattamento delle registrazioni particolari: registri e modalità di gestione

Non sono presenti registri specifici

7.6 – Politiche di sicurezza

POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATICO

1.1 Premessa

1. L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

2. Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

3. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

1.2 Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

3. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati della/e ditta/e < *inserire nome* > , includendo tutto il personale affiliato con terze parti.

2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

1.4 Politiche – Uso generale e proprietà

1. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.

2. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità

dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.

3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.

4. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.

5. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

1.5 Politiche Sicurezza e proprietà dell'informazione

1. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.

2. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.

3. Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in *stand-by* con un comando specifico.

4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.

5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.

6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.

7. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.

8. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

9. Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

2 Politiche Antivirus

2.1 Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.
I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.
I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

2.2 Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

2.3 Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

2.4 Politiche per le azioni preventive

- Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.
- Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.
- Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.
- Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.
- Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.
- Non scaricare mai messaggi da siti o sorgenti sospette.
- Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.
- Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.
- Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.
- Evitare collegamenti diretti ad Internet via modem.
- Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.

Firmato digitalmente da Frighetto Iole Antonella

• Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.

• Non utilizzare i server di rete come stazioni di lavoro.

• Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.

• Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

• Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.

• Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.

• I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).

• Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico… [omissis]…che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".

• Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

• È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

2.5 Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

• verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;

• verificare se il virus ha diffuso dati;

• identificare il virus;

• attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;

• installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;

• diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

3 Politiche Uso non accettabile

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

3. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.

2. Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.

3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.

4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.

5. Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.

6. Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.

7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.

8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.

9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:

a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione, b. attività di "sniffing";

c. disturbo della trasmissione;

d. spoofing dei pacchetti;

e. negazione del servizio;

f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;

g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.

11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.

12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.

13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.

14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).

2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.

3. Uso non autorizzato delle informazioni della testata delle e-mail,

4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.

5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.

6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

4 Linee telefoniche commutate (analogiche e digitali)

4.1 Scopo

1. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).

2. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

4.2 Ambito di applicazione

1. Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.

2. Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è

predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.

3. Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

4.4 Politiche – Telefax

1. Dovrebbero essere adottate le seguenti regole:

• le linee fax dovrebbero essere approvate solo per uso istituzionale;

• nessuna linea dei telefax dovrebbe essere usata per uso personale;

2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.

3. Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.

2. Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

4.6 Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:

• una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;

• lo scopo istituzionale per cui si rende necessaria la linea commutata;

• il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;

• che cosa la connessione esterna richiede per essere acceduta.

5 Politiche per l'inoltro automatico di messaggi di posta elettronica

5.1 Scopo

1. Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

5.2 Ambito di applicazione

Firmato digitalmente da Frighetto Iole Antonella

1. Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

5.3 Politiche

1. Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
2. Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

6 Politiche per le connessioni in ingresso su rete commutata

6.1 Scopo

1. Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.

6.2 Ambito di applicazione

1. Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

6.3 Politiche

1. Il personale dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di sfida/risposta (challenger/response).

2. È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive.

3. Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.

4. Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

7 Politiche per l'uso della posta istituzionale dell'amministrazione

7.1 Scopo

1. Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

7.2 Ambito di applicazione

1. La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

7.3 Politiche – Usi proibiti

1. Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

7.4 Politiche – Uso personale

1. È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:

- i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
- venga utilizzata una ragionevole quantità di risorse pubbliche;
- non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.

3. L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.

4. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

8 Politiche per le comunicazioni wireless

8.1 Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.

2. Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

8.2 Ambito di applicazione

1. La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.

2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i “punti di accesso” o le “stazioni base” collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.

2. Questi dispositivi sono soggetti a periodiche “prove di penetrazione” e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

8.4 Politiche – Approvazione delle tecnologie

1. Tutti i dispositivi di accesso alle LAN dell’Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

Firmato digitalmente da Frighetto Iole Antonella

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

Protocollo e data vedi segnatura in alto

OGGETTO: DECRETO DI ADOZIONE DEL MANUALE PER LA GESTIONE DEI FLUSSI DOCUMENTALI

IL DIRIGENTE SCOLASTICO

VISTI i sotto riportati provvedimenti

D.P.R. 445/2000 e ss mm	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
D.Lgs. 42/2004 e ss mm	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022);
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
D.Lgs. 196/2003 e ss mm	Codice in materia di protezione dei dati personali;

D.Lgs. 82/2005 e ss mm	Codice dell'amministrazione digitale (CAD);
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
Regolamento UE 910/2014 (Regolamento eIDAS)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

ESAMINATA LA DOCUMENTAZIONE trasmessa con la nota congiunta Ministero dell'Istruzione e Ministero della Cultura Prot. 3868 del .10.12.2021

DISPONE L'ADOZIONE

dell'allegato MANUALE PER LA GESTIONE DEI FLUSSI DOCUMENTALI.

IL DIRIGENTE SCOLASTICO
Dott.ssa Iole Antonella Frighetto

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

Protocollo e data vedi segnatura in alto

OGGETTO: DECRETO DI ADOZIONE DEL MASSIMARIO DI CONSERVAZIONE E SCARTO

IL DIRIGENTE SCOLASTICO

VISTI i sotto riportati provvedimenti

D.P.R. 445/2000 e ss mm	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
D.Lgs. 42/2004 e ss mm	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022);
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
D.Lgs. 196/2003 e ss mm	Codice in materia di protezione dei dati personali;

D.Lgs. 82/2005 e ss mm	Codice dell'amministrazione digitale (CAD);
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
Regolamento UE 910/2014 (Regolamento eIDAS)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

ESAMINATA LA DOCUMENTAZIONE trasmessa con la nota congiunta Ministero dell'Istruzione e Ministero della Cultura Prot. 3868 del 10.12.2021

DISPONE L'ADOZIONE

del MASSIMARIO DI CONSERVAZIONE E SCARTO (all. 2).

IL DIRIGENTE SCOLASTICO
Dott.ssa Iole Antonella Frighetto

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

Protocollo e data vedi segnatura in alto

OGGETTO: DECRETO DI ADOZIONE DEL TITOLARIO DI CLASSIFICAZIONE

IL DIRIGENTE SCOLASTICO

VISTI i sotto riportati provvedimenti

D.P.R. 445/2000 e ss mm	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA);
D.Lgs. 42/2004 e ss mm	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137;
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022);
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
D.Lgs. 196/2003 e ss mm	Codice in materia di protezione dei dati personali;

D.Lgs. 82/2005 e ss mm	Codice dell'amministrazione digitale (CAD);
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
Regolamento UE 910/2014 (Regolamento eIDAS)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

ESAMINATA LA DOCUMENTAZIONE trasmessa con la nota congiunta Ministero dell'Istruzione e Ministero della Cultura Prot. 3868 del 10.12.2021

DISPONE L'ADOZIONE

del TITOLARIO DI CLASSIFICAZIONE (all. 2).

IL DIRIGENTE SCOLASTICO
Dott.ssa Iole Antonella Frighetto

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

Liceo Scientifico "Da Vinci" ARZIGNANO

Registro dei trattamenti

Titolare del trattamento

Nome: Liceo Scientifico “Da Vinci” Arzignano
Email: vips08000d@istruzione.it
Pec: vips08000d@pec.istruzione.it
Telefono: 0444676125

Responsabile della protezione dati

Nome: MARCO BABOLIN
Email: dpo@robyone.net
Pec: dpo.robyone@ronepec.it
Telefono: 0490998416

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I
Via Fontis A. 2 - 36071 Arzignano (VI)
Tel.: 0444676125 - Mail: vips08000d@istruzione.it - PEC: vips08000d@pec.istruzione.it

Indice dei contenuti

1 Acquisti 3
2 Contabilità e Patrimonio 3
3 Gestione Alunni 3
4 Gestione Immagini e Video 4
5 Gestione Risorse Umane 4
6 Inserimento Alunni 5
7 Descrizione generale delle misure di sicurezza tecniche e organizzative 5

Firmato digitalmente da Frighetto Iole Antonella

1 Acquisti

Finalità

Pubblicità, Gestione dei fornitori, Monitoraggio degli adempimenti contrattuali, Adempimento di obblighi fiscali e contabili

Categorie di interessati

Fornitori Esterni / Professionisti, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Azienda di servizi

Categorie di dati personali

Attività economiche, commerciali, finanziarie e assicurative, Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Indirizzo e-mail e numero cellulare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare

Categorie di destinatari

Amministrativo generico, Amministratore di sistema, Delegato - Direttore dei Servizi Generali Amministrativi, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Banche e istituti di credito, Altre amministrazioni Pubbliche, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

10 anni dopo il termine del contratto

2 Contabilità e Patrimonio

Finalità

Gestione del patrimonio mobiliare e immobiliare, Gestione dei fornitori, Trattamento giuridico ed economico del personale, Monitoraggio degli adempimenti contrattuali, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizioni a sindacati o all'esercizio di diritti sindacali

Categorie di interessati

Dipendenti, Fornitori Esterni / Professionisti, Familiari

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare, Coordinate bancarie, Attività economiche, commerciali, finanziarie e assicurative

Categorie di destinatari

Amministrativo generico, Amministratore di sistema, Amministrativo personale, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Enti locali, Banche e istituti di credito, Altre amministrazioni Pubbliche, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

Come da normativa vigente

3 Gestione Alunni

Finalità

Istruzione e assistenza scolastica

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I
Via Fornis A., 3 - 36074 Arzignano (VI)
Tel.: 0444676125 - Mail: vips08000d@istruzione.it - PEC: vips08000d@pec.istruzione.it

Categorie di interessati

Alunno, Familiari

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Istruzione, Stato di salute - patologie attuali, Stato di salute - terapie in corso, Codice fiscale ed altri numeri di identificazione personale, Dati relativi alla famiglia o a situazioni personali, Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc., Indirizzo e-mail e numero cellulare, Stato di salute - altro, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Carte sanitarie

Categorie di destinatari

Collaboratore scolastico, Amministratore di sistema, Docente, Amministrativo didattica, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Enti locali, Istituti, scuole e università, Enti previdenziali ed assistenziali, Altre amministrazioni Pubbliche, Imprese di assicurazione, Associazioni e cooperative

Termini ultimi previsti per la cancellazione

Come da normativa vigente

4 Gestione Immagini e Video

Finalità

Attività promozionali

Categorie di interessati

Alunno

Categorie di dati personali

Immagini, Fotografie

Categorie di destinatari

Dipendenti, Amministratore di sistema, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Familiari

Termini ultimi previsti per la cancellazione

Per un anno dopo il termine del contratto per le foto individuali, per le foto di gruppo illimitata

5 Gestione Risorse Umane

Finalità

Trattamento giuridico ed economico del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Monitoraggio degli adempimenti contrattuali, Igiene e sicurezza del lavoro, Gestione del personale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizioni a sindacati o all'esercizio di diritti sindacali

Categorie di interessati

Dipendenti

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Iscrizione a sindacato, Codice fiscale ed altri numeri di identificazione personale, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Istruzione, Indirizzo e-mail e numero cellulare, Stato di salute - altro, Idoneità al lavoro, Dati relativi alla famiglia o a situazioni personali, Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc., Attività economiche, commerciali, finanziarie e assicurative, Coordinate bancarie, Immagini, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Carte sanitarie

Categorie di destinatari

Amministratore di sistema, Amministrativo personale, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Banche e istituti di credito, Intermediari finanziari, Istituti, scuole e università, Enti previdenziali ed assistenziali, Altre amministrazioni Pubbliche, Organizzazioni sindacali e patronati, Imprese di assicurazione, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

Illimitata

6 Inserimento Alunni

Finalità

Istruzione e assistenza scolastica

Categorie di interessati

Alunno, Familiari

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Dati relativi alla famiglia o a situazioni personali, Istruzione

Categorie di destinatari

Amministratore di sistema, Docente, Amministrativo didattica, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Altre amministrazioni Pubbliche, Imprese di assicurazione

Termini ultimi previsti per la cancellazione

Come da normativa vigente

7 Descrizione generale delle misure di sicurezza tecniche e organizzative

- **Accordi di riservatezza o di non divulgazione**

  I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati
- **Apparecchiature incustodite degli utenti**

  Gli utenti devono assicurare che le apparecchiature incustodite siano appropriatamente protette
- **Backup delle informazioni**

  Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata
- **Cessazione o variazione delle responsabilità durante il rapporto di lavoro**

  Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o al collaboratore e resi effettivi

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I
Via Fornis A, 3 - 36074 Arzignano (VI)
Tel.: 0444676125 – Mail: vips08000d@istruzione.it – PEC: vips08000d@pec.istruzione.it

- **Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni**

  Tutto il personale dell'organizzazione e, quando pertinente, il collaboratore, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa
- **Controlli contro il malware**

  Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
- **Controlli di accesso fisico**

  Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi
- **Controlli di rete**

  Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni. Firewall, VLAN, eccetera.
- **Disponibilità delle strutture per l'elaborazione delle informazioni**

  Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità
- **Disposizione delle apparecchiature e loro protezione**

  Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato
- **Infrastrutture di supporto**

  Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari
- **Inventario degli asset**

  Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato
- **Limitazione dell'accesso alle informazioni**

  L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi
- **Limitazioni all'installazione del software**

  Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti
- **Log di amministratori e operatori**

  Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente
- **Manutenzione delle apparecchiature**

  Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità
- **Messaggistica elettronica**

  Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato
- **Politica di controllo degli accessi**

  Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni
- **Politica per i dispositivi portatili**

  Deve essere adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di dispositivi portatili
- **Politiche per la sicurezza delle informazioni**

  Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti
- **Processo disciplinare**

  Deve essere istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni
- **Protezione contro minacce esterne ed ambientali**

  Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti
- **Rimozione o adattamento dei diritti di accesso**

  I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione

Firmato digitalmente da Frighetto Iole Antonella

VIPS08000D - AXOG19S - REGISTRO PROTOCOLLO - 0006404 - 27/06/2025 - I.1 - I
Via Fornis A., 3 - 36074 Arzignano (VI)
Tel.: 0444676125 – Mail: vips08000d@istruzione.it – PEC: vips08000d@pec.istruzione.it

- **Ruoli e responsabilità per la sicurezza delle informazioni**

  Tutte le responsabilità relative alla sicurezza delle informazioni dovrebbero essere definite e assegnate
- **Segregazione nelle reti**

  Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi
- **Sicurezza dei cablaggi**

  I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti
- **Sincronizzazione degli orologi**

  Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento
- **Sistema di gestione delle password**

  I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità
- **Termini e condizioni di impiego**

  Gli accordi contrattuali con il personale e con i collaboratori devono specificare le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni
- **Trattamento degli asset**

  Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione
- **Utilizzo accettabile degli asset**

  Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate. Regole al personale anche relative a: uso dei dispositivi portatili, BYOD, scrivania pulita, schermo pulito, trasporto (p.e. dei documenti cartacei), blocco dei pc quando non usati, eccetera.

Firmato digitalmente da Frighetto Iole Antonella

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)

C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

OGGETTO: Decreto per la costituzione di un gruppo di lavoro per l'aggiornamento del manuale di gestione documentale alla luce delle più recenti Linee Guida AGID sulla formazione, gestione e conservazione dei documenti e del massimario.

IL DIRIGENTE SCOLASTICO

VISTO il Regio Decreto 02 ottobre 1911 n.1163 recante "Regolamento per gli archivi di Stato";

VISTO il Decreto del Presidente della Repubblica 30 settembre 1963 n.1409 recante "Norme relative all'ordinamento ed al personale degli archivi di Stato";

VISTA la Legge 7 agosto 1990 n.241 recante "Nuove norme sul procedimento amministrativo";

VISTO il Decreto del Presidente della Repubblica 28 dicembre 2000 n.445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";

VISTO il Decreto del Presidente della Repubblica 08 gennaio 2001 n.37 recante "Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato";

VISTO il DPCM 31 ottobre 2000 recante "Regole tecniche per il protocollo informatico";

VISTO il Decreto legislativo 30 giugno 2003 n.196 recante "Codice in materia di protezione dei dati personali";

VISTO il Decreto legislativo 22 gennaio 2004 n.42 recante "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137";

VISTA la Legge 9 gennaio 2004 n.4 e ss.mm.ii. recante "Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici";

VISTO l'art.71 del Decreto legislativo 7 marzo 2005 n. 82 recante "Codice dell'amministrazione digitale";

VISTA la Legge 18 giugno 2009 n. 69 recante "Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile";

VISTO il Decreto legislativo 30 dicembre 2010 n. 235 recante "Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69";

VISTO il DPCM 3 dicembre 2013 recante "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";

Firmato digitalmente da Frighetto Iole Antonella

VISTA la Legge 7 agosto 2015 n. 124 recante "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche";

VISTO il Decreto legislativo 26 agosto 2016 n. 179 recante "Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche";

VISTE le:

a) Linee guida del 23 marzo 2018 sulla caratterizzazione dei sistemi cloud per la pubblica amministrazione;

b) Linee guida 23 marzo 2018 per la marcatura dei documenti normativi secondo gli standard norme in rete;

c) Linee guida del 23 marzo 2018 per il Disaster Recovery (DR) delle PA;

d) Linee guida del 11 aprile 2019 sull'Indice delle Pubbliche Amministrazioni;

e) Linee guida del 13 maggio 2019 su acquisizione e riuso di software per le pubbliche amministrazioni;

f) Linee guida del 20 giugno 2019 sulle Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate v.1.1;

g) Linee guida del 20 aprile 2020 per il rilascio dell'identità digitale per uso professionale;

h) Linee guida del 21 aprile 2020 sul RAO pubblico;

i) Linee guida del 23 aprile 2020 per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD;

l) Linee guida del 07 maggio 2020 sulla sicurezza informatica, relative agli allegati 1-2-3-4;

m) Linee guida del 18 settembre 2020 sull'accessibilità degli strumenti informatici;

n) Linee guida del 18 maggio 2021 sul documento informatico e relativi allegati;

o) Linee guida del 22 ottobre 2021 sull'interoperabilità tecnica delle Pubbliche Amministrazioni;

p) Linee guida del 22 ottobre 2021 sulle Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici;

q) Linee guida del 22 ottobre 2021 sull'INAD;

r) Linee guida del 19 novembre 2021 sul punto di accesso telematico ai servizi della Pubblica Amministrazione;

VISTA la nota 3868 del 10 dicembre 2021 recante "Messa a disposizione di nuovi strumenti a supporto della gestione documentale delle Istituzioni scolastiche" con cui il Ministero dell'Istruzione ed il Ministero della Cultura hanno ridefinito, in collaborazione con AGID, il modello di gestione documentale delle Istituzioni scolastiche;

RITENUTO necessario istituire un gruppo di lavoro che consenta l'adozione di un manuale di gestione documentale sulla base del modello proposto dal Ministero e conforme alle sopraccitate linee guida AGID anche attraverso una revisione dell'organizzazione e delle procedure adottate per lo svolgimento delle attività amministrative e didattiche.

CONSIDERATO che allo scopo di cui al precedente punto possono contribuire, con le loro esperienze e competenze, le seguenti figure facenti parte dell'organigramma d'istituto:

a) il Direttore del Servizi Generali e Amministrativi;

b) gli assistenti tecnici, componenti dell'Ufficio Tecnico, in servizio presso l'istituto;

c) l'assistente amministrativo addetto al protocollo e alla pubblicazione albo pretorio, in servizio presso questo Istituto;

d) l'animatore digitale dell'Istituto;

VERIFICATA la disponibilità delle predette figure alla partecipazione al gruppo di lavoro;

DISPONE

A partire dal 01/01/2024 e fino a compimento dei lavori è istituito il gruppo citato in parola. Tale gruppo di lavoro avrà i seguenti compiti:

a) coadiuvare il dirigente scolastico nell'analisi delle linee guida AGID citate in premesse;

b) predisporre un manuale di gestione documentale dell'istituto nel rispetto delle suddette linee guida anche attraverso una revisione dell'organizzazione e delle procedure adottate per lo svolgimento delle attività amministrative e didattiche

c) predisporre un piano di adeguamento del sistema informatico dell'istituto alle procedure di digitalizzazione indicate nelle suddette linee guida da sottoporre ai competenti Organi collegiali della scuola per le necessarie deliberazioni.

IL DIRIGENTE SCOLASTICO

DOTT.SSA IOLE ANTONELLA FRIGHETTO

LICEO SCIENTIFICO "DA VINCI"
ARZIGNANO
Segreteria didattica 0444/676125 – 670599
Segreteria amministrativa 0444/672206
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 94024870241
Codice meccanografico vips08000d
e-mail: vips08000d@istruzione.it - pec: vips08000d@pec.istruzione.it - sito: www.liceoarzignano.edu.it

Protocollo e data vedi segnatura in alto

IL DIRIGENTE SCOLASTICO

VISTI I SOTTO RIPORTATI PROVVEDIMENTI

D.P.R. 445/2000 e successive modificazioni	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA)
D.Lgs. 42/2004 e successive modificazioni	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137[1]
Linee Guida AgID	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate dall'AgID con Determinazione n. 407/2020 del 9 settembre 2020 ed in seguito aggiornate con Determinazione n. 371/2021 del 17 maggio 2021 (da attuare entro il 1° gennaio 2022)
L. 241/1990	Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
D.Lgs. 196/2003 e successive modificazioni	Codice in materia di protezione dei dati personali
D.Lgs. 82/2005 e successive modificazioni	Codice dell'amministrazione digitale (CAD)
DPCM del 22 febbraio 2013	Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71
DPCM del 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni
Regolamento UE 910/2014 (Regolamento *eIDAS*)	Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

ESAMINATA LA DOCUMENTAZIONE trasmessa con la nota congiunta Ministero dell'Istruzione e Ministero della Cultura Prot. 3868 del 10.12.2021
SENTITO il Direttore dei Servizi Generali ed Amministrativi

DISPONE LA SEGUENTE ORGANIZZAZIONE DELLE UNITA' ORGANIZZATIVE RESPONSABILI (UOR)

UOR 1: AMMINISTRAZIONE – LEGALE – PATRIMONIO - CONTABILITA'
UOR 2: PERSONALE
UOR 3: DIDATTICA

Il Dirigente scolastico
Dott.ssa Iole Antonella Frighetto

All.: ut supra