

2019

REGOLAMENTO GDPR



D.P. O. Roberto De Duro, Andrea Caristi,

Corrado Faletti

Scuola XXXXX

01/01/2019

Sommario

PARTE PRIMA: INTRODUZIONE.....	4
PREMESSA DI CARATTERE NORMATIVO	4
PREMESSA DI CARATTERE ORGANIZZATIVO.....	5
PREMESSA DI CARATTERE METODOLOGICO	6
PARTE SECONDA DISPOSIZIONI GENERALI.....	7
OGGETTO DEL REGOLAMENTO	7
FINALITÀ' DEL REGOLAMENTO	7
SENSIBILIZZAZIONE.....	7
DEFINIZIONI	8
PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI.....	9
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI).....	10
TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI).....	10
COMUNICAZIONE DI DATI VERSO L'ESTERNO	11
PARTE TERZA DIRITTI DELL'INTERESSATO	12
INFORMATIVA SUL TRATTAMENTO DEI DATI.....	12
CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI	13
DIRITTO DI ACCESSO DELL'INTERESSATO.....	20
DIRITTO DI RETTIFICA	23
DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO).....	23
DIRITTO DI LIMITAZIONE AL TRATTAMENTO.....	24
DIRITTO ALLA PORTABILITÀ' DEI DATI.....	24
DIRITTO DI OPPOSIZIONE	24
PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)	25
PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO.....	26
TITOLARE DEL TRATTAMENTO	26
CONTITOLARI DEL TRATTAMENTO.....	27
RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI.....	27
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI.....	29
AUTORIZZATO INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI	30
RESPONSABILE DELLA PROTEZIONE DEI DATI.....	31
PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO	34
PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA.....	34
REGISTRO ELETTRONICO DELLE ATTIVITÀ' DI TRATTAMENTO	34

PROTEZIONE E SICUREZZA DEI DATI PERSONALI.....	34
NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO	35
VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI	36
TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO.....	36
DISCIPLINA SULLA VIDEOSORVEGLIANZA.....	36
DISCIPLINA SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI.....	36
PARTE SESTA ATTUAZIONE IN AMBITO SCOLASTICO DEGLI ADEMPIMENTI EUROPEI ..	37
AMBITI DI ATTIVITA' CORRELATI AI NUOVI OBBLIGHI EUROPEI	37
ENTRATA IN VIGORE E PUBBLICITA'	38
DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'	38

PARTE PRIMA: INTRODUZIONE

PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta "privacy") è uno strumento di applicazione del nuovo **Regolamento Europeo n. 2016/679**, nell'ambito dell'organizzazione dell'Istituto Omnicomprensivo Formicola Liberi Pontelatone di Formicola.

A far data dal 25 maggio 2018 trova diretta applicazione, sul territorio nazionale, l'anzidetto, nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

La sua entrata in vigore è stabilita il 24 maggio 2016: entro due anni a partire da tale data, e quindi entro la data del 25 maggio 2018, tutti gli Stati membri dell'Unione dovevano uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche sia di natura penale) previste dalla nuova normativa.

La data del 25 maggio 2018 è inderogabile, in quanto le prescrizioni stabilite dal Regolamento di cui si tratta trovano diretta ed immediata applicazione, indipendentemente dalla preesistenza di differenti norme nazionali in materia che, quindi, sono automaticamente superate dai precetti del Regolamento n. 2016/679.

Ciò comporta che le disposizioni legislative di cui ex Codice della privacy (*D.lgs. 196/2003 e ss.mm.ii.*), così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, siano superate, a far data dal 25.05.2018, da quelle del Regolamento UE, nella misura in cui le norme nazionali siano contrastanti o incompatibili con quelle europee e vengono integrate dal Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679 – GDPR.

Il presente Regolamento si rende inoltre necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali (*D.lgs. 196 del 30/06/2003, regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*).

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

PREMESSA DI CARATTERE ORGANIZZATIVO

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge alla struttura scolastica, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questa SCUOLA, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza ed alla implementazione del "processo di umanizzazione" in corso di realizzazione, nell'ambito di questa SCUOLA, oramai da molti anni.

Link di interesse

www.istomnicomprensivoformicola.edu.it

www.garanteprivacy.it

www.istomnicomprensivoformicola.edu.it/index.php/privacy

Ai sensi del Nuovo Regolamento Europeo sulla Privacy entrato in vigore il 25 maggio 2018 (GDPR), si comunicano i dati di riferimento dei referenti e si rinvia alla pagina del sito istituzionale <http://istomnicomprensivoformicola.edu.it/index.php/privacy> dove è pubblicata l'informativa completa. Qualsiasi approfondimento può essere svolto sul sito del garante al seguente indirizzo www.garanteprivacy.it oppure tramite la mail protocollo@pec.gpdp.it

Titolare del trattamento: Istituto Omnicomprensivo Formicola Liberi Pontelatone) rappresentato dal dirigente scolastico Prof.ssa Antonella TAFURI	Numero di telefono: 0823876016 Indirizzo email: ceic8a8008@istruzione.it
Responsabile Protezione Dati (RPD): Corrado Faletti - Servizi e Supporti s.r.l.	Indirizzo email: direttore@controllerprivacy.it

PREMESSA DI CARATTERE METODOLOGICO

Vengono allegati a questo Regolamento una serie di **documenti tecnici** necessari a dare compiuta attuazione, sia verso l'interno che verso l'esterno, ai dettami della nuova "privacy europea": documenti ai quali viene data massima pubblicità e diffusione, tramite la pubblicazione sullo spazio internet.

Tra questi documenti vi sono, a titolo esemplificativo, il modello di accordo per la nomina del Responsabile esterno del trattamento dei dati personali, il modulo per l'informativa ed il consenso al trattamento dei dati, ed il disciplinare sull'utilizzo dei mezzi informatici e telematici della Scuola.

E' doveroso infatti rimarcare, sin da ora, che il principio cardine introdotto dal nuovo Regolamento UE è quello della "**responsabilizzazione**" (**accountability** nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "**conformità**" o **compliance** nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Questa SCUOLA, nella persona del Suo Dirigente Scolastico, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* ed alla *compliance*.

PARTE SECONDA DISPOSIZIONI GENERALI

OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno della scuola Istituto Omnicomprensivo Formicola Liberi Pontelatone, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

FINALITÀ' DEL REGOLAMENTO

La Scuola garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

SENSIBILIZZAZIONE

La Scuola sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con la Scuola.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento, al momento dell'ingresso in servizio è fornita, a cura della Segreteria, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente, esperto esterno*) una specificazione comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (*o nella lettera di incarico per i soggetti non dipendenti poc' anzi citati*), con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali “**autorizzati al trattamento dei dati**” ai sensi del Regolamento UE 2016/679.

Detta comunicazione conterrà anche i riferimenti per reperire il presente Regolamento sul sito internet.

Il Regolamento, pubblicato sul sito, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare si intende per:

- a) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- b) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- c) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- d) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- e) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- f) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- g) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- h) **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- i) **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- l) **«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- m) **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- n) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- o) **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- p) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le “definizioni” su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre “definizioni” si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (*«liceità, correttezza e trasparenza»*);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»).

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).

Come stabilito dal Regolamento UE, il Titolare del trattamento (Scuola nella persona del Dirigente Scolastico della Scuola) è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'«**accountability**» o «**responsabilizzazione**»).

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche*, le *convinzioni religiose o filosofiche*, o l'*appartenenza sindacale*, nonché trattare *dati genetici*, *dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare con le "*Autorizzazioni generali*", dall'Autorità Garante per la protezione di dati personali.

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, "*il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.*"

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati giudiziari e

in particolare con le “*Autorizzazioni generali*”, dall’Autorità Garante per la protezione di dati personali.

COMUNICAZIONE DI DATI VERSO L’ESTERNO

La comunicazione di dati sensibili e giudiziari da parte di un soggetto pubblico ad altro soggetto pubblico è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

PARTE TERZA DIRITTI DELL'INTERESSATO

INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni**:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- d) il diritto di proporre reclamo a un'autorità di controllo;
- e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- f) l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questa SCUOLA, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, si fa rinvio al vigente **Prontuario (Massimario) di conservazione e scarto**, pubblicato sul sito internet di questa SCUOLA e liberamente consultabile.

Per prontuario (massimario) di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette di gestire in modo organizzato l'archivio, permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

Alla luce dei principi esposti, si rinvia al documento allegato n. 5 (*“Modulistica relativa all’informativa e al consenso al trattamento dei dati”*) del presente Regolamento, ove è prodotto sia il modello di **“Informativa”** che quello di raccolta del **“consenso”**, sia che ciò avvenga nei confronti di persone adulte e capaci, che di soggetti minori ed incapaci.

CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'ideale base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy (*consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati*).

In particolare:

- per i dati **“sensibili”** il consenso deve essere **“esplicito”** (si veda art. 9 regolamento): lo stesso dicasi per il consenso a decisioni basate su **trattamenti automatizzati** (compresa la profilazione, articolo 22);
- **non deve essere necessariamente “documentato per iscritto”**, né è richiesta la **“forma scritta”**, anche se questa è modalità idonea a configurare inequivocabile accettazione del consenso e il suo essere **“esplicito”** (per i dati sensibili); inoltre, il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;
- Il **consenso dei minori** è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (articolo n. 8 del Regolamento Europeo); qualora non sia inteso (il consenso) come raccolta per utilizzo di strumenti dell'informazione (es. goggle app, registri elettronici, social, etc.) allora lo stesso può essere anche raccolto solo per i minori di 14 anni.

- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare “caselle pre-spuntate” su un modulo);
- deve essere manifestato attraverso “**dichiarazione o azione positiva inequivocabile**” (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Interesse vitale di un terzo: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46 del Regolamento UE).

Interesse legittimo prevalente di un titolare o di un terzo:

- Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell’interessato non spetta all’Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del **principio di “responsabilizzazione”** introdotto dal nuovo pacchetto protezione dati;
- l’interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell’interessato per costituire un valido fondamento di liceità;
- il regolamento chiarisce espressamente che l’interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

DIRITTO DI ACCESSO DELL’INTERESSATO

Come stabilito dall’articolo n. 15 del Regolamento Europeo n. 2016/679, l’interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere **l’accesso** ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l’esistenza del diritto dell’interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un’ autorità di controllo;
- g) qualora i dati non siano raccolti presso l’interessato, tutte le informazioni disponibili sulla loro origine;
- h) l’esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all’articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l’importanza e le conseguenze previste di tale trattamento per l’interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

I principi suesposti sono recepiti anche nel testo dell'allegato 5 del presente Regolamento, ove è prodotto sia il modello di "**Informativa**" che quello di raccolta del "**consenso**", sia che ciò avvenga nei confronti di persone adulte e capaci, che di soggetti minori ed incapaci.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il **diritto di accesso**, si fa rinvio alle vigenti disposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale e regionale nonché dal Garante per la privacy, con particolare riferimento all'ambito scolastico.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "**accesso documentale**", di "**accesso civico**" e di "**accesso generalizzato**".

Nel dare evidenza del fatto che, presso questa SCUOLA, la competenza sulla materia *de quo* è affidata al **Responsabile della Trasparenza e della Prevenzione della Corruzione**, si rinvia al contenuto delle *schede informative* pubblicate sul **sito internet**, dedicate all'argomento.

A tale riguardo, nel rinviare a quanto pubblicato al sito web, si fa presente che:

- a) per **accesso documentale** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti della Scuola, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184).

Possono fare domanda tutti i cittadini portatori di un interesse "*diretto, concreto e attuale*,

corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso" (art. 22, Legge 241/1990).

Per presentare domanda, è necessario rivolgersi alla Servizio/Ufficio o Struttura che detiene il documento di cui si chiede l'accesso, portando con sé il proprio documento di identità valido.

I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono quelle previste dal *tariffario* pubblicato sul sito web.

Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).

- b) per *accesso civico* si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 "*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche*", e Decreto Legislativo 33 del 14/03/2013: "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*").

La richiesta viene presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza della SCUOLA utilizzando il modulo prodotto sul sito internet.

La Scuola, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, la Scuola indica al richiedente il relativo collegamento ipertestuale.

Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

- c) per *accesso generalizzato* si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto *Freedom of Information Act* o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

La richiesta viene presentata:

- a) all'Unità che detiene i dati, le informazioni o i documenti;

b) all'Ufficio Relazioni con il Pubblico utilizzando il modulo pubblicato sul sito internet.

Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali controinteressati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato.

Se il documento risulta già pubblicato nel sito nel rispetto della normativa vigente, la Scuola indica al richiedente il relativo collegamento ipertestuale.

Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio"**, che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata**.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri

dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al “blocco” del trattamento di cui all’art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l’interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell’art. 21 del regolamento (in attesa della valutazione da parte del titolare).**

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze (*consenso dell’interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante*).

Il diritto alla limitazione prevede che il dato personale sia “**contrassegnato**” in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

DIRITTO ALLA PORTABILITA’ DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell’interessato o sulla base di un contratto stipulato con l’interessato (quindi non si applica ai dati il cui trattamento si fonda sull’interesse pubblico o sull’interesse legittimo del titolare, per esempio), e solo i dati che siano stati “forniti” dall’interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall’interessato, se tecnicamente possibile.

DIRITTO DI OPPOSIZIONE

Come stabilito dall’articolo n. 21 del Regolamento Europeo n. 2016/679, l’interessato ha il **diritto di opporsi in qualsiasi momento**, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell’articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione**, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO

Il **"Titolare"** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è la Scuola, nella persona del suo Dirigente Scolastico, in qualità di legale rappresentante della Scuola stessa, con sede in *Via Cantiello, 11 – 81040 – Formicola (CE)*.

Il Titolare, avvalendosi della supervisione e collaborazione del *Data Protection Officer* provvede:

- a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
- b) a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali*, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- c) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
- d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- e) a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (*accountability* nell'accezione inglese) di titolari e responsabili, ovvero sulla adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in

particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questa SCUOLA, nella persona del Suo Dirigente Scolastico, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* sin dalla adozione della Deliberazione n. 86 del 24.01.2018 relativa alle "prime azioni" utili ad ottemperare alle previsioni legislative di matrice europea.

CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento**. Essi determinano in modo trasparente, mediante un *accordo interno*, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI

Secondo il codice europeo 679/2016, s'intende per Responsabile del trattamento dei dati, *"la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali"*.

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno", questa SCUOLA, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, come sempre avvenuto in passato presso la SCUOLA, continuare a designare in ambito i **Responsabili interni del trattamento dei dati personali**, conferendo l'incarico a quei dipendenti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Nell'ambito della SCUOLA, vengono quindi individuati quali **Responsabili interni del trattamento dei dati personali**:

- per la presidenza i professori Di Gaetano Antonietta, Fusco Anna e Missana Roberta;
- per la funzione di segreteria i sig.ri Di Camillo Luigi (Dsga) e Scirocco Carmela (A.A.);
- per le attività delle funzioni strumentali i professori De Matteo M.Grazia, Di Dario Velia, Di Gaetano Antonietta, Fusco Anna, Izzo Maria, Lombardi Mirella, Merola Rosa, Monaco Pasqualina, Rotondo Rosa e Santagata Michelina;
- per le attività di orientamento i professori Cacace Mariangela e Izzo Maria;
- per le attività di supporto alla disabilità i professori Di Gaetano Antonietta e Isolda Emilia;
- per le attività di gestione informatica Di Gaetano Antonietta, Fusco Anna, Missana Roberta.

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Responsabile interno del trattamento deve:

- 1) trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento nonché le specifiche istruzioni impartite dal Titolare;
- 2) garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
- 3) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
- 4) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;
- 5) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
- 6) contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il Responsabile per il trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il **Data Protection Officer (DPO)**, al fine di:

- a) comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti.*
- b) utilizzare il modello di *Informativa e Consenso* approvato con il presente Regolamento, verificandone il

- rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;
- c) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
 - d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati della Scuola siano applicate all'interno della Scuola stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
 - e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Questa SCUOLA provvederà, contestualmente all'approvazione con atto deliberativo del Dirigente Scolastico del presente Regolamento, alla **nomina dei Responsabili interni del trattamento dei dati**, dandone comunicazione personale a ciascun Responsabile all'uopo nominato.

RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito della SCUOLA, sono inoltre individuati quali **Responsabili "esterni" del trattamento dei dati personali**, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con la SCUOLA, trattino dati di cui è titolare la SCUOLA medesima e qualora siano in possesso dei requisiti in precedenza previsti dall'articolo 29, primo comma, del Codice della privacy (esperienza, capacità ed affidabilità).

In ottemperanza al nuovo **articolo 28 del Regolamento Europeo 2016/679**, i Responsabili esterni hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, degli studenti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con la SCUOLA e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento";
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;

- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (*sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati*), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso la Scuola, il Responsabile Esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante "accordo di nomina" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente alla Scuola.

In allegato al presente Regolamento vengono quindi prodotti il **"format" di accordo di nomina** del Responsabile del trattamento esterno con relative **istruzioni per lo svolgimento dell'incarico**, oltre al **"format" di lettera di trasmissione** (*all'Ente interessato nonché, per conoscenza, al Data Protection Officer*) del succitato accordo di nomina.

Dopo l'approvazione del presente Regolamento, la UOC Affari Generali provvederà a trasmettere il presente Regolamento a tutte le strutture interessate, evidenziando la necessità di provvedere alle nomine dei Responsabili esterni utilizzando la nuova modulistica sin qui citata ed allegata al presente Regolamento.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

AUTORIZZATO INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI

Il Regolamento Europeo si sofferma sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere *"autorizzato"* al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente o titolare di borsa di studio*) una specificata

comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali “**autorizzati al trattamento dei dati**” ai sensi del Regolamento UE 2016/679.

Detta comunicazione conterrà anche i riferimenti per reperire il presente Regolamento sul sito internet.

Il Regolamento, pubblicato sul sito, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

Analoghe considerazioni valgono per la figura **autorizzato esterno**: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa SCUOLA, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima (*quali consulenze, collaborazioni o borse di studio conferite dalla SCUOLA*), devono essere designati da parte del Responsabile (in questo caso “esterno”) tramite una lettera (o una nota) di nomina come *autorizzati esterni*.

Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno della Scuola in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario) per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato o di sostegno.

Nel caso di autorizzati esterni, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del **Data Protection Officer** (in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come **attività principali i dati sensibili su larga scala**, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in **conflitto di interessi** in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il *consulente* ed il *revisore* e non dovrebbe ricoprire ruoli gestionali rispetto all'attività della Scuola o ai fini istituzionali della Pubblica Amministrazione.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- ✓ **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;

- ✓ **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- ✓ collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;
- ✓ **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**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

2. **adempire alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle dipendenze del titolare oppure sulla base di un contratto di servizio (RPD esterno);
4. **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempire ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Ente dei **“dati di contatto” del RDP**: dati che debbono essere inseriti anche nell'informativa sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese **“data protection by default and by design”**, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*“sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso”*, secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa SCUOLA verrà gestito in via digitale e sarà esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

Per tale motivo, anche questa SCUOLA, per mezzo dei competenti servizi dell'area informatica, è impegnata a compiere i passi necessari per gestire tale registro elettronico.

PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva (*“tra le altre, se del caso”*).

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere obblighi generalizzati di adozione di misure “minime” di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi

specificamente individuati come da art. 32 del regolamento.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" del vecchio Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Per le modalità organizzative con le quali questa SCUOLA ha stabilito di ottemperare all'adempimento sin qui descritto, vale il presente regolamento e l'obbligo di predisporre le più idonee misure di sicurezza a livello informatico, adeguando le misure minime e valutandone gli impatti, anche curando l'aggiornamento (e/o la riedizione) del **Documento Programmatico sulla Sicurezza (D.P.S.)**.

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

Il Titolare deve **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *"senza ingiustificato ritardo"*, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di *"Data Breach"*.

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre *"senza ingiustificato ritardo"*; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Il Titolare del trattamento, sentito il Data Protection Officer, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (<http://www.garanteprivacy.it/web/quest/home/docweb/-/docweb-display/docweb/1915835>) che intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento.

Il predetto modello è allegato al presente Regolamento.

VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell’art. 32 è una lista aperta e non esaustiva (“tra le altre, se del caso”).

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**.

Quest’ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All’esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l’autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l’Autorità non avrà il compito di “autorizzare” il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell’articolo 58: dall’ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

TRASFERIMENTO DI DATI PERSONALI ALL’ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

DISCIPLINA SULLA VIDEOSORVEGLIANZA

Si fa rinvio alle disposizioni di cui al *Regolamento* tempo per tempo vigente, che disciplina la materia di cui si tratta.

DISCIPLINA SULL’UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

Si fa rinvio alle disposizioni di cui al *Regolamento* tempo per tempo vigente, che disciplina la materia di cui si tratta.

PARTE SESTA ATTUAZIONE IN AMBITO SCOLASTICO DEGLI ADEMPIMENTI EUROPEI

AMBITI DI ATTIVITA' CORRELATI AI NUOVI OBBLIGHI EUROPEI

1. Gestione della comunicazione interna ed esterna

La comunicazione interna ed esterna è di pertinenza della Presidenza ed è autorizzata dal Dirigente Scolastico dopo attenta valutazione dei contenuti.

2. Utilizzo di strumenti informatici

Per la gestione degli strumenti informatici si rimanda all'apposito regolamento allegato al presente

3. Gestione dei social

L'utilizzo dei social (chat, blog, etc.) deve essere autorizzato espressamente dal Dirigente Scolastico che ne valuta gli eventuali impatti di concerto con il DPO.

4. Trasmissione dei dati personali ai Consigli di classe ai fini della personalizzazione delle attività didattiche

Qualora i consigli di classe abbiano la necessità di visionare dati sensibili legati ad eventuali piani didattici personalizzati gli stessi possono essere visualizzati tramite gli appositi strumenti informatici in dotazione all'Istituto (*Registro elettronico AXIOS*). Gli stessi non devono essere duplicati o archiviati in modo differente da quello utilizzato ufficialmente dalla Segreteria.

5. Utilizzo dei loghi e dell'immagine dell'Istituzione Scolastica

L'utilizzo di loghi o altri emblemi rappresentanti l'Istituzione Scolastica deve essere autorizzato dal Dirigente Scolastico

6. Video riprese e fotografie interne all'Istituto

Le riprese all'interno dei locali scolastici devono essere autorizzate e la loro riproduzione è soggetta al controllo dei contenuti.

7. Utilizzo di dati personali al di fuori degli strumenti informatici ufficiali (registro di classe, etc.)

È espressamente vietata la conservazione di copie di dati sensibili al di fuori degli strumenti forniti dall'Istituto (ad esempio su chiavette, copie nelle scrivanie, su pc personali).

8. Gestione delle Attività delle scuole con particolari esigenze

Per quanto riguarda le scuole agrarie, gli alberghieri e le gestioni conto terzi è necessario individuare le tipologie di trattamenti e definire appositi regolamenti.

9. Ingresso nelle classi di personale esterno

L'ingresso nelle classi di personale non autorizzato è severamente vietato senza l'autorizzazione del Dirigente. Qualora l'ingresso sia dovuto a motivi legati alla salute del bambino (terapie, controlli, verifica in loco, etc.) occorre che la richiesta sia approvata dal consiglio di classe e che tutti i genitori della classe sottoscrivano il consenso alla Privacy.

ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del Consiglio di Istituto.

Il Regolamento verrà pubblicato sul sito internet (nell'apposita, nuova sezione dedicata alla "privacy europea").

DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del Dirigente Scolastico, su indicazioni del DPO, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.

Gli eventuali aggiornamenti ai *documenti allegati* verranno, pertanto, inseriti in tempo reale sul sito internet nell'apposita sezione dedicata alla "privacy europea", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo della mail, così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

Esaurito il punto all'O.d.g. la seduta è tolta alle ore 10,30.



IL COMMISSARIO STRAORDINARIO

Genfraro Iannotta

D.S.



ISTITUTO OMNICOMPRESIVO FORMICOLA-LIBERI-PONTELATONE
VIA CANTIELLO - 81040 FORMICOLA (CASERTA)
Tel. 0823/876016 – Fax. 0823/876963
C.F. 93108530614 - C.M. CEIC8A8008
Comprende i Plessi di FORMICOLA- LIBERI – PONTELATONE-
STRANGOLAGALLI-VAL D'ASSANO
Codice Univoco di fatturazione: UFVI9G
e-mail: ceic8a8008@istruzione.it e-mail certificata: ceic8a8008@pec.istruzione.it
sito internet: <http://www.istomnicomprensivofornicola.edu.it/>



Allegato al Regolamento d'Istituto GDPR

REGOLAMENTO DI UTILIZZO DEGLI STRUMENTI INFORMATICI E DELLA CONNESSIONE AD INTERNET

rivolto a tutti i soggetti a vario titolo coinvolti nell'uso di strumenti e servizi (Docenti, personale amministrativo e tecnico e collaboratore scolastico, studenti e famiglie, collaboratori esterni fornitori o fruitori di servizi)

Premesse di buon comportamento

Tutti gli utenti che utilizzano internet devono rispettare:

- La legislazione vigente applicata alla comunicazione su internet
- La netiquette (etica e norme di buon uso dei servizi di rete)

Tutte le parti chiamate in causa dal presente documento devono leggerlo attentamente per accertarsi di averlo compreso in tutte le sue parti e di recepirne i contenuti.

I vantaggi di internet a scuola

Il curriculum scolastico prevede che **gli studenti** imparino a reperire materiale, recuperare documenti e scambiare informazioni attraverso l'uso delle TIC. Internet offre sia agli studenti sia al **personale docente** una vasta scelta di risorse e opportunità di scambi culturali con persone di altri paesi. Inoltre, su internet si possono recuperare risorse su tempo libero, attività scolastiche e sociali, proposte collaborativo-lavorative.

La scuola propone, sia agli studenti sia al personale docente, di utilizzare internet al fine di promuovere l'eccellenza in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Per gli studenti ed il personale docente l'accesso ad internet è un privilegio ed un diritto. L'accesso ad internet permette al personale docente di svolgere in modo agevole ed efficace diverse funzioni rilevanti da un punto di vista professionale, in primo luogo l'autoaggiornamento e la partecipazione ad iniziative di e-learning avviate dal Ministero. La possibilità di accedere da scuola alle risorse documentarie tramite internet diviene un fattore imprescindibile per lo svolgimento della professione e per un uso corretto ed efficace delle nuove tecnologie per la didattica.

L'accesso ad internet diventa per gli allievi uno strumento di acquisizione del sapere che si affianca agli strumenti tradizionali e lo rende implicitamente oggetto di particolare attenzione per la formazione dei giovani. L'approccio all'uso delle TIC si presenta quindi come ambito formativo non esclusivamente disciplinare ma trasversale rispetto all'azione educativa dell'istituto.

Esiste però la possibilità che gli studenti trovino materiale inadeguato ed illegale su internet; a tal proposito l'istituto deve prendere opportune precauzioni, limitando l'accesso a internet. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on line, di stabilire obiettivi chiari nell'uso di internet e di insegnarne un uso accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare

le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli studenti.

Per il **personale ATA**, oltre alle attività legate alle proprie mansioni (trasmissioni telematiche al ministero, monitoraggio progetti, utilizzo della piattaforma di segreteria, etc), l'utilizzo di internet è consentito e promosso per tutte quelle attività legate all'aggiornamento e formazione del proprio profilo professionale.

Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni necessarie per garantire il divieto di accesso a materiale inappropriato, anche se non è possibile evitare che nessuno si trovi di fronte a materiale inadatto navigando su un computer della scuola.

La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dalla navigazione. Gli studenti imparano ad utilizzare i metodi di ricerca su internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Ricevere e inviare informazioni o messaggi e-mail prevede una buona abilità di gestione delle informazioni e di comunicazione. Le abilità di gestione delle informazioni includono:

- garanzia di validità, la diffusione e l'origine delle informazioni a cui si accede o che si ricevono;
- utilizzazione di fonti alternative di informazione per proposte comparate;
- ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e dei possibili altri link al sito;
- rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e ad evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli studenti non deve essere sottoposto materiale di questo tipo e se ne venissero casualmente a contatto dovrebbero sempre riferire l'indirizzo internet (URL) ai responsabili.

Inoltre, l'utilizzo di internet comporta una serie di rischi che possono avere ripercussioni sulla gestione degli archivi sia di dati comuni sia sensibili:

- rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati;
- rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker;
- rischio interno dovuto ad intrusioni da parte di studenti;
- rischio interno/esterno di scaricamento di virus, Trojan e worm tramite posta elettronica e/o operazioni di download.

Le strategie della scuola per garantire la sicurezza sull'uso delle TIC

La rete didattica dell'istituto è fisicamente separata dalla rete amministrativa; la rete didattica è protetta da firewall e dotata di proxy server e filtro per la selezione dei contenuti.

La connessione ad internet della scuola è accessibile dopo essersi autenticati inserendo il proprio nome utente e la propria password; gli studenti devono chiudere la sessione dopo aver terminato il proprio lavoro.

Il sistema informatico dell'istituto è regolarmente controllato dai responsabili in base alle norme di sicurezza e/o per prevenire disfunzioni di tipo hardware/software.

Il personale controlla periodicamente i file utilizzati, i file di report, i file temporanei ed i siti internet visitati.

E' vietato inserire file sul server tranne che in apposite cartelle condivise; è vietato scaricare da internet software non autorizzati.

E' vietato il download di files : è considerato download di file lo scaricamento di materiale digitale da internet o supporti in genere (compresi mini disk, memorie sd, pen drive etc.).

Per utilizzare Pen Drive, CD ROM o altri supporti di memorizzazione personali è necessario chiedere un permesso e sottoporli a controllo antivirus; durante le attività, gli studenti non possono utilizzare file eseguibili (salvo gli applicativi di comune utilizzo) e utilità di sistema.

In generale, il software utilizzabile è solo quello autorizzato dalla scuola.

I file di proprietà dell'istituto sono posti in particolari aree del server soggette a protezione e vengono periodicamente controllati dal personale.

Il sistema informatico della scuola è provvisto di software antivirus aggiornato. Gli assistenti tecnici sono tenuti a vigilare sulla protezione dei sistemi. Ogni utente che importi dati a scuola tramite supporti esterni è tenuto a verificare l'assenza di virus nel proprio supporto.

La scuola pone in atto le misure preventive in suo possesso, ma ogni utente è informato che, considerata la vastità della problematica, esiste il pericolo reale di infettare il proprio supporto sul sistema della scuola, di conseguenza la scuola declina ogni responsabilità da ogni incidente che possa verificarsi da un eventuale infezione da virus.

Il sistema di accesso su internet prevede un filtro per evitare l'accesso a siti web con contenuto illegale e/o pornografico. Il sistema, installato su una stazione Linux che utilizza la distribuzione IpCop con funzioni di proxy e filtraggio contenuti, dà la possibilità di impedire l'accesso a siti non appropriati, consentire l'accesso

esclusivamente ad un numero limitato di siti approvati, monitorare i siti visitati dagli studenti e dai docenti.

Dopo un certo numero di violazioni delle regole stabilite dalla politica scolastica, l'istituto ha il diritto di eliminare l'accesso dell'utente ad internet per un certo periodo di tempo o in modo permanente.

Il personale che opera sulle TIC controllerà l'efficacia del sistema di filtraggio. A tal proposito, la strategia della scuola dipende dalle indicazioni previste dal curriculum e dall'età degli studenti in una classe.

Servizi di posta elettronica

Gli studenti durante le attività didattiche non possono utilizzare il servizio e-mail personale se questo interferisce con altre attività di apprendimento. In altri momenti scolastici possono accedere al servizio e-mail personale previa richiesta ai responsabili delle TIC.

Per tutti gli utilizzatori di internet è consentita la consultazione della propria e-mail personale se su dominio istituzionale, istruzione, trampi etc. Non è garantita la consultazione della propria e-mail su dominio privato in quanto potrebbero essere presenti materiali e/o servizi non conformi al presente regolamento.

Un indirizzo e-mail può essere attribuito ad un gruppo di studenti o ad una classe nel caso di attività didattiche che prevedano scambio di informazioni con altri gruppi di studenti o classi nell'ambito di una precisa programmazione di una disciplina.

Gli studenti devono riferire al docente o ai responsabili delle TIC se ricevono e-mail offensive; è vietato utilizzare catene telematiche di messaggi senza il permesso del mittente; gli studenti che leggono i propri messaggi sul server dei servizi di posta non devono lasciarne traccia sui computer dell'istituto; non è consentito configurare un client di posta locale per la lettura di e-mail né al personale docente né agli allievi; solo in casi particolari e in presenza di una ben precisa programmazione di disciplina, i responsabili delle TIC potranno configurare un client di posta locale per la lettura di e-mail al fine di favorire scambi culturali; gli studenti non devono rivelare dettagli o informazioni personali loro o di altre persone di loro conoscenza come indirizzi, numeri di telefono od organizzare incontri fuori dalla scuola.

Gestione del sito della Scuola

La redazione editoriale della scuola gestisce le pagine del sito ed è sua responsabilità garantire che il contenuto sul sito sia accurato ed appropriato. Il sito assolverà alle linee guida sulle pubblicazioni della scuola. La scuola detiene i diritti d'autore dei documenti che si trovano sul sito, oppure richiede il permesso all'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare devono includere solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il numero di telefono della scuola ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere.

Mailing list con moderatore, gruppi di discussione, chat rooms

L'istituto può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale. L'insegnante è il moderatore degli altri mezzi di collaborazione, di mailinglist, di gruppi di discussione e di chat rooms se questi sono utilizzati a scuola. Agli studenti non è consentito l'accesso alle chat rooms, salvo in casi particolari e in presenza di una ben precisa programmazione di disciplina sotto la responsabilità del docente; sono permesse solo chat a scopi didattici; la supervisione del docente è comunque necessaria per garantire la sicurezza; solo i gruppi di discussione che hanno obiettivi e contenuti didattici sono disponibili agli studenti.

Attacchi esterni

Sono considerati attacchi esterni tutte quelle attività legate ad individuare vulnerabilità dei sistemi interni o esterni alla scuola e ad utilizzarle per prendere il controllo totale o parziale, per arrecare danni, o solamente per avere accesso a dati non resi volontariamente pubblici. La scuola vieta espressamente tale tipologia di attività.

Servizi on line agli utenti esterni

All'interno del proprio sito web, la scuola offre servizi alle famiglie e agli utenti esterni:

- consultazione elenchi libri di testo;
- orari delle classi, dei docenti, degli uffici e delle strutture;
- comunicazioni alle famiglie;
- modulistica;
- tramite l'accesso al sito del registro elettronico, valutazioni degli allievi (accesso riservato all'utenza tramite nome utente e password personali).

Tali servizi sono erogati in conformità con quanto espresso della Legge 196/2003 in materia del trattamento dei dati.

Informazioni per gli studenti

Le regole di base relative all'accesso ad internet descritte nel presente documento saranno esposte nei laboratori di informatica, insieme al regolamento sull'uso delle TIC, e pubblicate sul sito della scuola.

Gli studenti saranno informati che l'utilizzo di internet è monitorato e verranno loro date le istruzioni per un uso responsabile e sicuro di internet.

Gli studenti e i loro genitori / tutori devono prendere visione del presente documento.

Informazioni per i genitori / tutori

I genitori / tutori vengono informati delle regole dell'uso internet dell'istituto sul sito web della scuola. Essi potranno richiedere una copia del documento; è auspicabile che le regole sull'uso accettabile e responsabile di internet all'interno dell'istituto siano condivise e conseguite dalle famiglie anche nell'ambiente domestico.

Eventuali commenti o suggerimenti connessi possono essere inviati all'attenzione del Dirigente Scolastico.

Informazioni per il personale scolastico

Il personale scolastico viene informato delle regole dell'accesso ad internet dell'istituto sul sito web della scuola. Esso potrà richiedere una copia del documento; è inoltre consapevole che l'uso di internet verrà monitorato e segnalato e che tutto il personale scolastico sarà coinvolto nello sviluppo del regolamento di utilizzo della rete della scuola e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di internet.

In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente scolastico o il responsabile delle TIC per evitare malintesi. Gli insegnanti saranno inoltre provvisti di informazioni concernenti le problematiche sul diritto d'autore che vengono applicate alla scuola.

REGOLAMENTO UTILIZZO SISTEMI INFORMATIVI

Art. 1 Oggetto e ambito di applicazione

Il presente regolamento e le sue premesse che ne sono parte integrante, disciplinano le modalità di accesso, di uso delle risorse informatiche dell'Istituto dell'Istituzione scolastica (rete, apparecchiature e risorse infrastrutturali, patrimonio informativo e software).

Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati. Le risorse software sono i sistemi operativi e i programmi acquisiti legalmente dall'Istituto).

Il presente regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alla rete della scuola: impiegati amministrativi, tecnici, docenti, collaboratori scolastici e alunni. Si applica anche a taluni utenti esterni, quali i collaboratori esterni, ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, ditte fornitrici di hardware o delegate alla sua manutenzione (è consentita la visualizzazione di files solo per quanto strettamente indispensabile), eventuali enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse.

Art. 2 Principi generali – Diritti e Responsabilità

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. Tutti i soggetti interagenti, a qualunque titolo, col sistema informatico dell'Istituto sono anche responsabili di eventuali danni erariali conseguenti.

Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione in files-registro; la registrazione riguarda orario di inizio e fine dell'accesso al sistema e all'account che ha operato. Detti files possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo; possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal DLgs. n. 196/2003 e normativa collegata.

L'Istituto, per fini legati alla sicurezza dell'intero sistema informativo, dispone di strumenti per il monitoraggio e il controllo della navigazione in internet.

Art. 3 Utilizzo dei personal computer

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività professionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Pertanto:

- a) L'uso dell'elaboratore con profilo di accesso specifico (utenti dell'area Amministrativa e di Sistema, Sistema integrato del registro elettronico, piattaforma di e-Learning, account individuali riservati) deve essere protetto da password e non divulgata. Gli account destinati al trattamento di dati amministrativi e sensibili sono custoditi a cura del Titolare del trattamento dati.
- b) I preposti all'amministrazione del sistema, nell'espletamento delle funzioni legate alla sicurezza e alla manutenzione informatica, avranno la facoltà di accedere in qualunque momento anche da remoto a tutte le postazioni e a tutti gli account.
- c) Il personal computer deve essere spento **al termine dell'orario delle lezioni o di servizio**, comunque prima di lasciare gli uffici, i laboratori di informatica, le aule. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Al termine di qualunque sessione riservata di lavoro o di assenza temporanea è obbligatorio uscire dall'account o bloccare il computer.
- d) L'accesso ai dati presenti nel personal computer di area amministrativa potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato;
- e) è vietato installare autonomamente programmi informatici sui server salvo autorizzazione esplicita degli amministratori di sistema, e sui Pc salvo autorizzazione del Titolare, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore;
- f) è vietato modificare le caratteristiche impostate sul proprio Pc, salvo con autorizzazione esplicita degli amministratori di sistema o del Titolare;
- g) è vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate agli amministratori di sistema;
- h) È vietata l'installazione sul proprio Pc di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa degli amministratori di sistema o del Titolare. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente gli amministratori di sistema o Titolare nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Art. 4 Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità.

In presenza di reti locali con dominio, i files relativi alla produttività individuale possono essere salvati sul server e i limiti di accesso sono regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti aventi profili di autorizzazione diversi.

Gli amministratori di sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui Pc degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.

Costituisce buona regola la periodica **pulizia degli archivi**, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Pc se non strettamente necessarie (e per breve tempo) allo scambio dei file con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di minare la sicurezza dell'intero sistema.

È compito degli amministratori di sistema provvedere alla creazione e alla manutenzione di aree condivise sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica È fatto divieto di:

- a)** Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;
- b)** Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- c)** Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
- d)** Installare componenti hardware non compatibili con l'attività istituzionale;
- e)** Rimuovere, danneggiare o asportare componenti hardware;
- f)** Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti;
- g)** Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e piú in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- h)** Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 5 Utilizzo di internet

I Pc abilitati alla navigazione in Internet costituiscono uno strumento necessario e prezioso per lo svolgimento dell'attività professionale.

Nell'uso di internet e della posta elettronica non sono consentite le seguenti attività:

- a)** L'uso di internet per motivi personali (ad esempio facebook).
- b)** L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
- c)** Lo scaricamento (download) di software e di file non necessari all'attività istituzionale, sia perchè potrebbero celare minacce al buon funzionamento del sistema, sia perchè software privi di licenza comportano gravissime sanzioni economiche e penali per il Datore di lavoro ed eventualmente anche per il dipendente;
- d)** Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
- e)** Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali;
- f)** Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Il dipendente non deve eseguire download di files eseguibili o documenti da siti Web, HTTP o FTP non conosciuti. Si ricorda che la frequentazione di siti non conosciuti o lo scaricamento di files da fonti non garantite possono introdurre virus o altro malware, che possono creare inconvenienti gravissimi, con perdita di dati, blocco operativo e danni economici importanti. L'imprudente autore può essere chiamato a risponderne in via disciplinare e per il danno recato.

Art. 6 Utilizzo della posta elettronica

La casella di posta assegnata dall'Istituto, è uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.

È fatto divieto di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Direttore SGA, o in ogni caso opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.

Per la trasmissione di files all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 MB È preferibile utilizzare le cartelle di rete condivise).

è obbligatorio controllare i file attachments (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

In particolare nell'uso della posta elettronica non sono consentite le seguenti attività:

- a) La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali e inerenti le ragioni di servizio;
- b) L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
- c) Inviare tramite posta elettronica informazioni quali user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

Art. 7 Utilizzo delle password

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono previste ed attribuite dai referenti di sistema, ovvero dal Titolare del trattamento dei dati.

è necessario procedere alla modifica della password almeno ogni tre mesi (come previsto dal disciplinare tecnico allegato al Codice della privacy, GDPR n.679/2016) con contestuale comunicazione all'Incaricato della custodia delle Password.

La comunicazione di variazione delle password di accesso ai servizi amministrativi dovrà avvenire secondo la modulistica prevista dal Titolare e dovrà essere consegnata al "Custode delle password", in busta chiusa, con data, nome e firma dell'incaricato apposte sul lembo di chiusura.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (disciplinare tecnico Privacy). La password dev'essere modificata ogni 3 mesi se il computer consente l'accesso a dati sensibili, altrimenti ogni 6 mesi. La password non deve essere scritta su supporti cartacei.

Nel caso si sospetti che la password abbia perso la segretezza, deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle Password,

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

Art. 8 Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD e DVD) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (disciplinare tecnico Privacy). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (disciplinare tecnico Privacy) devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili e DVD) obsoleti devono essere consegnati agli Amministratori di Sistema per l'opportuna distruzione.

Ogni qualvolta si procederà alla dismissione di un Personal Computer gli Amministratori di Sistema provvederanno alla distruzione o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 9 Utilizzo di p.c. portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, lavoro domestico autorizzato, ecc...), in caso di allontanamento devono essere custoditi in un luogo protetto.

Art. 10 Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non-adatti (molto lunghi o non supportati, come ad esempio files di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

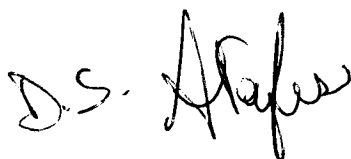
Art. 11 Osservanza delle disposizioni in materia di Privacy

è obbligatorio attenersi alle disposizioni in materia di Privacy del GDPR 679/2016 e alle misure minime di sicurezza previste, come indicate nella lettera di designazione di RESPONSABILE del trattamento dei dati.

Art. 12 Amministratori di Sistema

Gli Amministratori di Sistema sono i soggetti cui è conferito il compito di sovrintendere alle risorse informatiche dell'Istituto e a cui sono consentite le seguenti attività:

- a) Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
- b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica istituzionale, secondo le direttive impartite dal Titolare;
- c) Utilizzare le credenziali conservate dal "Custode delle password" oppure le credenziali di accesso di amministrazione del sistema o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Titolare per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
- d) Solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, eseguire le seguenti attività:
 - 1) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi;
 - 2) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, attesa l'autorizzazione del Titolare;
 - 3) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti;
 - 4) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti.



La legge sul diritto d'autore

Negli ultimi 15 anni, a partire dalla direttiva 91/250/CEE relativa alla tutela del software, la spinta dell'Unione europea è stata determinante in materia di diritto d'autore al fine di evitare differenze ed incertezze normative negli stati membri. Anche nell'ordinamento italiano tali disposizioni comunitarie sono state recepite mediante una serie di decreti (D.Lgs. 6 maggio 1999, n. 169, "Attuazione della Direttiva 96/9/CE relativa alla tutela giuridica delle banche dati"; D.Lgs. 2 febbraio 2001, n. 95, "Attuazione della Direttiva 98/71/CE relativa alla protezione giuridica dei disegni e dei modelli"; D.Lgs. 9 aprile 2003, n. 68, "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione") che, di fatto, hanno aggiornato la Legge 22 aprile 1941, n. 633 (la cosiddetta "Legge sul diritto d'autore").

La legge sul diritto d'autore tutela:

1. le opere letterarie;
2. le opere musicali;
3. le opere coreografiche e pantomimiche;
4. le opere delle arti figurative;
5. i disegni e le opere dell'architettura;
6. le opere dell'arte cinematografica;
7. le opere fotografiche;
8. i programmi per elaboratore;
9. le banche di dati;
10. il disegno industriale /design.

Il diritto d'autore nasce con la creazione dell'opera stessa; vi sono due categorie di diritti tutelati:

- diritti morali, non cedibili a terzi (essere riconosciuto autore dell'opera, mantenere l'opera inedita, opporsi a modifiche);
- diritti patrimoniali, cedibili a terzi e che si estinguono dopo 70 anni dalla morte dell'autore (riproduzione in esemplari, comunicazione e distribuzione, noleggio e prestito, diffusione via etere).

La "Legge sul diritto d'autore" tutela sia da un punto civile (art. 156 e seguenti) sia da un punto di vista penale (art. 171 e seguenti) le opere.

Tutte le opere dell'ingegno pubblicate su internet (testi, immagini, musica, ...) e i siti web, qualora siano creazioni intellettuali nuove ed originali, sono tutelate dalla "Legge sul diritto d'autore"; chi realizza l'opera ha "il diritto di utilizzare economicamente l'opera in ogni forma e modo, originale e derivata".

La condivisione tra utenti di opere protette dal diritto d'autore "anche mediante programmi di condivisione di file tra utenti [...] mediante reti e connessioni di qualsiasi genere" è stata, a partire da quest'anno, oggetto di un intervento legislativo (il cosiddetto Decreto Urbani).

La Legge 21 marzo 2004, n. 128, con cui è stato convertito il D.L. 22 marzo 2004, n. 72 (detto Decreto Urbani) è finalizzata a contrastare la diffusione telematica abusiva di opere dell'ingegno. Le disposizioni più significative stabiliscono che:

- il reato di duplicazione e diffusione abusiva di opere dell'ingegno viene punito qualora sia commesso per trarne profitto;
- in tale delitto è compreso espressamente l'uso della tecnologia peer-to-peer, quando non sia per uso personale;
- è necessario versare a favore della SIAE un "compenso" sul prezzo di supporti ottici e dei software di masterizzazione;
- nel caso in cui un'opera dell'ingegno venga pubblicata on-line, è obbligatorio fornire un avviso sull'avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi;
- gli Internet Service Provider (ISP) hanno l'obbligo, su ordine dell'autorità giudiziaria, di rimuovere i contenuti dei siti che violano la normativa in esame, pena una sanzione amministrativa da € 50.000 a € 250.000 per chi non coopera.

