



**ISTITUTO COMPRENSIVO AD INDIRIZZO MUSICALE**  
**SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI I GRADO "DON BOSCO"**

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                     |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  | <p>Scuola Primaria - Via Platania, n°13 - Tel. 0925/61162<br/>Scuola dell'infanzia e Primaria - Imbornone, n°1 - Tel. 0925/540424<br/>Scuola Media Navarro - Via Imbornone, SNC - Tel. 0925/61281<br/><b>C.F:83002130843 Cod. Univoco UFT4T8</b><br/>e-mail: <a href="mailto:agic85600x@istruzione.it">agic85600x@istruzione.it</a> pec: <a href="mailto:agic85600x@pec.istruzione.it">agic85600x@pec.istruzione.it</a> sito web:<br/><a href="http://www.icdonboscoribera.edu.it">www.icdonboscoribera.edu.it</a></p> |  |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|

**REGOLAMENTO SULL'USO DI INTERNET E DELLA POSTA ELETTRONICA**  
**MESSA A DISPOSIZIONE DEI DIPENDENTI**  
**PER L'ESERCIZIO DELLE FUNZIONI D'UFFICIO**  
**(POLICY DELLA SCUOLA)**

*Triennio scolastico 2022/2025*

*Approvato dal Collegio dei Docenti n. 3 del 18/09/2023*

*Approvato dal Consiglio di Istituto n. 2 del 29/09/2023*

**Il presente Regolamento è parte integrante del PTOF 2022/2025**

**AGGIORNAMENTO ANNO SCOLASTICO 2024/25**

## INDICE

|                                                                     |         |
|---------------------------------------------------------------------|---------|
| Premesse generali .....                                             | Pag. 3  |
| Art. 1 – Definizioni .....                                          | Pag. 5  |
| Art. 2 – Finalità .....                                             | Pag. 5  |
| Art. 3 – Ambito di applicazione .....                               | Pag. 5  |
| Art. 4 – Principi fondamentali .....                                | Pag. 5  |
| Art. 5 – Compiti dell’Amministratore di Sistema .....               | Pag. 6  |
| Art. 6 - Accesso ad Internet e uso della rete scolastica .....      | Pag. 6  |
| Art. 7 – Uso del sistema della posta elettronica .....              | Pag. 7  |
| Art. 8 – Memorizzazione file log durante la navigazione .....       | Pag. 7  |
| Art. 9 – Controlli .....                                            | Pag. 8  |
| Art. 10 – Assistenza tecnica da remoto .....                        | Pag. 8  |
| Art. 11 – Provvedimenti disciplinari .....                          | Pag. 9  |
| Art. 12 – Data Breach .....                                         | Pag. 9  |
| Art. 13 – Soluzioni che garantiscono la continuità lavorativa ..... | Pag. 10 |
| Art. 14 – Informativa .....                                         | Pag. 10 |
| Art. 15 - Prescrizioni interne .....                                | Pag. 10 |

**REGOLAMENTO SULL'USO DI INTERNET E DELLA POSTA ELETTRONICA  
MESSO A DISPOSIZIONE DEI DIPENDENTI  
PER L'ESERCIZIO DELLE FUNZIONI D'UFFICIO  
(POLICY AZIENDALE)**

**Premessa generale**

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso delle tecnologie telematiche sia conformato al rispetto dei diritti fondamentali, nonché della dignità dell'interessato.

Occorre ulteriormente premettere che:

- a) compete ai dirigenti scolastici (datori di lavoro) assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- c) emerge l'esistenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinato ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- d) l'utilizzo di internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante l'elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *email* e l'archiviazione di messaggi) di controllo che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
- e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

**Premesse particolari:**

**Viste** la legge 7 agosto 1990 n. 241 *“Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”* e la Legge 11 febbraio 2005 *“Modifiche ed integrazioni alla legge 7/8/90 n. 41 concernenti norme generali sull’azione amministrativa”*;

**Visto** il D. Lgs. 19/03/96 *“modifiche e integrazioni al D. Lgs. n. 626/1994 controlli operati tramite sistemi aziendali”*;

**Visto** il DPR del 28/12/2000 n. 445 *“Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”*

**Visto** il D. Lgs. del 30/06/2003 n. 196 *“Codice in materia di protezione di dati personali”* e sue s.m.i.;

**Visto** il D.M. del 7 dicembre 2006, n. 305 *“Regolamento recante identificazione dei dati sensibili e giudiziari”*

**Vista** la deliberazione del CNIPA 19/12/2004 n. 11 *“Regole tecniche dei documenti digitali”*;

**Visto** il D. Lgs. 7 marzo 2005 n. 82 *“Codice dell’Amministrazione Digitale”*;

**Visto** il S.O. n. 93 aggiornato dal D. Lgs. 159 del 4/4/2006 recante *“Disposizioni integrative e correttive al D. Lgs. 7/3/2005 n. 82”*

**Vista** la legge 20 maggio 1970 n. 300 *“Statuto dei Lavoratori”*;

**Vista** la Direttiva del Consiglio dei Ministri n. 2/2009 del 26/05/2009;

**Ritenuto** opportuno richiamare gli artt. 2086, 2087 e 2014 del Codice Civile;

**Considerato** che l’istituto Comprensivo “Don Bosco” tra i vari strumenti di lavoro, ha messo a disposizione dei dipendenti accessi ad Internet (laboratori di informatica) e servizi di caselle di posta elettronica per lo svolgimento delle mansioni e compiti loro affidati;

**Richiamato** il principio generale che l’utilizzo delle risorse TIC che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza e correttezza e normalmente adottati nell’ambito dei rapporti di lavoro;

**Rilevato** che l’Autorità Garante per la Privacy, con delibera n. 13 del 1.3.2007 (pubblicato in G.U. del 10.3.2007 n. 58) ha inteso precisare che è opportuno da parte dei Datori di Lavoro, adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato verso i singoli dipendenti interessati, anche ai fini dell’esercizio del potere disciplinare;

**Ritenuto** che l’adozione del regolamento consente di escludere l’applicabilità della normativa penale a tutela della corrispondenza elettronica poiché, essendo considerata strumento di lavoro, non può essere considerata corrispondenza privata;

*POLICY AZIENDALE*

**Considerato**, inoltre, che, se correttamente applicato e fatto rispettare, il regolamento può risultare uno efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa della Scuola;

**Ritenuto**, pertanto dover adottare apposito **Regolamento per l'utilizzo di Internet e della Posta Elettronica** in cui è tra l'altro, precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai commi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali d. lgs. 196/2003 n. 196 e del D.M. 35 del 7 dicembre 2006;

**Tenuto conto** che il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori, interni od esterni, della scuola, agli esperti esterni, ai collaboratori a progetto, a prescindere dal rapporto contrattuale con la stessa intrattenuto;

**VISTO** il Regolamento europeo 2016/679 nell'art. 15 e negli artt. dal 16 sino al 22;

## **Art. 1 – Definizioni**

a) L'Istituzione Scolastica si identifica con l'istituto Comprensivo "Don Bosco";

b) "Utenti":

- l'insieme dei soggetti interni (personale amministrativo, docenti, collaboratori scolastici, esperti esterni), che indipendentemente dal rapporto di lavoro intrattenuto con l'amministrazione scolastica, utilizzano, nella loro attività lavorativa, connessioni ad Internet e sistema di posta elettronica;
- le ditte che effettuano attività di manutenzione, gli eventuali altri soggetti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle convenzioni stesse nel rispetto del presente regolamento.

## **Art. 2 – Finalità**

Il presente regolamento disciplina le modalità di accesso e di uso della Rete informatica, telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto Scolastico per dare il supporto informatico, documentario, alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

## **Art. 3 – Ambito di applicazione**

La Rete dell'Istituto Scolastico è costituita dall'insieme delle risorse informatiche, cioè:

- dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete informatica dell'Istituto;
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

#### **Art. 4 – Principi fondamentali**

Sono tenuti all'osservanza del presente disciplinare tecnico i "Responsabili del Trattamento" dei dati personali e gli "Incaricati del Trattamento" ai sensi del d. lgs. 196/2003, nonché i Responsabili e gli autorizzati al Trattamento "esterni" all'Istituto Comprensivo.

La navigazione in Internet e il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione di dati. I dati che vengono inviati e ricevuti con tale sistema sono di esclusiva proprietà dell'Istituzione Scolastica.

Tutte le attività svolte mediante la navigazione in Internet e il sistema di posta elettronica sono finalizzate al conseguimento dei fini istituzionali dell'Istituzione Scolastica.

La connessione ad Internet e il sistema di posta elettronica sono operativi con continuità nell'intervallo di tempo di apertura degli uffici di segreteria.

Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella di posta elettronica almeno una volta al giorno. Parimenti hanno l'obbligo di non cedere ad altri la propria password di cui sono gli unici responsabili e di sostituirla periodicamente nel rispetto del d. lgs. 196/2003 con le modalità ed i tempi in esso riportati.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi del Codice *Privacy*:

- a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai dipendenti;
- c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, osservando il principio di *pertinenza e non eccedenza*. Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "*mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza*";
- d) il principio di *indispensabilità* nel caso in cui ricorra il trattamento di dati sensibili.

## **Art. 5 – Compiti dell'Amministratore di Sistema**

L'abilitazione per la connessione ad Internet e il servizio di posta elettronica verranno gestiti dall'Amministratore di Sistema o da altra figura tecnicamente competente a cui sono assegnate la responsabilità del corretto funzionamento degli strumenti elettronici, del monitoraggio costante dei livelli dei sistemi al fine di garantire la massima efficienza, della storicizzazione dei processi, della realizzazione e conservazione delle copie di backup, nonché di assicurare l'assistenza tecnica e formativa degli utenti.

## **Art. 6 – Accesso ad Internet e uso della rete scolastica**

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete internet dai personal computer, espone la scuola a rischi di coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine della medesima.

L'utilizzo delle risorse informatiche e telematiche della scuola devono sempre ispirarsi al principio della diligenza e della correttezza, pertanto, la Scuola ha adottato il presente Regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Internet è una rete mondiale di computer che contiene milioni di pagine di informazioni; parte di queste possono avere contenuti offensivi o illegali, con cui si può entrare accidentalmente in contatto attraverso interrogazioni a motori di ricerca effettuate per scopi "innocui".

Pertanto la scuola non si ritiene responsabile per il materiale acceduto o scaricato da internet da parte degli utenti e cerca di minimizzare i rischi connessi all'uso di internet mediante l'applicazione di quanto contenuto nel presente Regolamento, cui gli utenti sono obbligati ad attenersi.

L'uso di Internet nelle numerose funzionalità è consentito esclusivamente per gli scopi attinenti alle proprie mansioni.

Per non limitare le attività tipicamente aziendali, non è definito a priori un elenco di siti autorizzati; è tuttavia permesso l'utilizzo di adeguati strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività lavorative.

Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Viene altresì proibita la possibilità di caricare/scaricare (upload/download) a/da Internet files musicali, video o software che non siano attinenti alla propria mansione, come anche l'utilizzo della connessione ad Internet per motivi strettamente personali, in quanto ciò si configura come danno

patrimoniale cagionato all'Amministrazione consistente nel mancato svolgimento della prestazione lavorativa durante il periodo di connessione.

Viene tassativamente vietato l'utilizzo delle risorse del server centrale per la memorizzazione di materiale privato, personale o non attinente alla attività lavorativa.

Relativamente all'utilizzo dei singoli PC affidati agli utenti, si precisa che l'assegnazione delle risorse non ne comporta la privatezza, in quanto trattasi di strumenti di esclusiva proprietà scolastica e quindi i files memorizzati non sono né tutelati né garantiti dall'Istituto Comprensivo, per qualsiasi causa.

Infine, il dipendente preposto all'utilizzo di internet nonché della posta elettronica è tenuto, comunque, ad osservare il segreto d'Ufficio ai sensi dell'art. 15 del D.P.R. 10.01.1957, n. 3

#### **Art. 7 – Uso di sistema di posta elettronica**

Sono attivati indirizzi di posta elettronica condivisi dagli operatori scolastici, assegnati a ciascuno per opportunità lavorativa del tipo nome.cognome@istruzione.it

La “personalizzazione” dell'indirizzo non comporta la sua “privatezza”, in quanto trattasi di strumenti di lavoro di esclusiva proprietà dell'istituto Comprensivo messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Non è ammesso l'utilizzo di alcun sistema di posta elettronica personale e/o privato in quanto ritenuto cagionevole per l'Amministrazione ai fini del rapporto qualità/tempo del servizio lavorativo prestato, anche fuori dall'orario di lavoro o durante le pause.

#### **Art. 8 – Memorizzazione files di log durante la navigazione internet**

Al fine di verificare la funzionalità, la sicurezza del sistema e il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, generano un registro, *log file*, (così come si creano anche i file temporanei e i *cookie*) contenente le informazioni relative ai siti che i singoli PC hanno visitato. Tale registro memorizza l'indirizzo fisico delle prestazioni di lavoro e non i riferimenti dell'utente garantendo in tal modo il suo anonimato.

L'accesso a questi dati è effettuato dal Dirigente Scolastico o da un suo fiduciario autorizzato *ad hoc*.

#### **Art. 9 – Controlli**

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Istituto Comprensivo “Don Bosco” effettuerà con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti

fasi, al fine di verificare l'effettivo adempimento delle prestazioni lavorative e, occorrendo, anche il corretto e legittimo utilizzo degli strumenti di lavoro:

1. analisi aggregata del traffico di rete riferita agli uffici di segreterie e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo alla osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
3. in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità verranno effettuati controlli sull'occupazione dello spazio di memorizzazione sul server centrale attraverso le fasi:

1. analisi aggregata dei dati memorizzati sul server a livello degli uffici di segreterie e rilevazione della tipologia di utilizzo (file audio, file video, immagini software non autorizzato) e relativa permanenza con l'attività lavorativa;
2. emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo alla osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
3. in caso di successivo permanere di una situazione non conforme, è possibile procedere con una analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

#### **Art. 10 – Assistenza tecnica da remoto**

In relazione alle eventuali attività di manutenzione da remoto ai PC delle segreterie connessi ad internet, il personale tecnico autorizzato dalla Istituzione scolastica potrà utilizzare specifici software. Tali programmi verranno utilizzati per assistere l'utente durante la normale attività informatica ovvero di svolgere manutenzione su applicazioni e su hardware. L'attività di assistenza e manutenzione avverrà previa autorizzazione telefonica da parte dell'utente interessato. La configurazione del software da utilizzare per gli interventi da remoto, prevedranno un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al PC.

Potrà essere fornita, su richiesta, una informativa sul software utilizzato, nonché le modalità del suo utilizzo per tutti gli utenti interessati.

### **Art. 11 – Provvedimenti disciplinari**

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimamente, nel rispetto dell'art. 4 comma 2 dello statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti. La lettura e la registrazione sistematica del servizio di accesso ad internet vengono automaticamente registrate. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su: numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione. Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il titolare del trattamento procede in forma graduata: in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti, se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, ...) o tipologie di utenti (ata, docenti, studenti, ...) e si procede con avvisi mirati alle categorie di utilizzatori, ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali, in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare nelle forme e con le modalità previste dall'istituto per gli studenti (vedere Regolamento di Istituto e di disciplina), dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente, può portare alle azioni civili e penali consentite. L'utilizzo dei servizi di accesso ad internet cessa o viene sospeso d'ufficio quando: non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso, vi è il sospetto di manomissione dell'hardware o del software, in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc. ..., in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati, -ogni qualvolta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

### **Art. 12 Data Breach**

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali e al cosiddetto data Breach.

Con il termine data breach si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali

*POLICY AZIENDALE*

all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- perdita accidentale: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
  - furto: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
  - infedeltà aziendale: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
  - accesso abusivo: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite
- **Il data breach nell'ordinamento giuridico italiano ed europeo**

Il Garante per la Protezione dei Dati Personali ha introdotto l'obbligo di avvisare l'autorità e gli utenti in caso di gravi violazioni a seguito di attacchi informatici o di eventi avversi (ad esempio incendi) che possano comportare la perdita, la distruzione o la diffusione indebita di dati.

In capo ai titolari dei trattamenti vige l'obbligo di condurre una preliminare ricognizione dei dati trattati e dei rischi ai quali sono soggetti cui dovrà seguire l'adozione di idonee misure di sicurezza.

La comunicazione della violazione al Garante deve avvenire in tempi molto rapidi e nei casi più gravi di violazioni è previsto l'obbligo di informare ciascun contraente coinvolto. La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza e sistemi di cifratura e di anonimizzazione che rendano inintelligibili i dati.

Per consentire l'attività di accertamento del Garante, occorre tenere un elenco aggiornato delle violazioni subite, con il dettaglio delle circostanze e delle conseguenze. L'inventario deve adottare misure che ne garantiscano integrità ed immutabilità.

- **Adempimenti previsti in caso di data breach**

In caso di violazione dei dati personali, il Garante ha adottato una serie di provvedimenti che prevedono l'obbligo di comunicazione. In caso di attacchi informatici, accessi abusivi, incidenti o eventi avversi (come ad esempio incendi) che determinano perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati, le aziende e la pubblica amministrazione deve operare come di seguito illustrato:

**Data breach per le amministrazioni pubbliche:** obbligo di comunicare entro 48 ore dalla conoscenza del fatto, con comunicazione tramite apposito modello tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

A tale proposito, è stato introdotto dall'articolo 33, l'obbligo generalizzato, in capo al titolare del trattamento di notifica di data breach all'autorità di controllo (DPO) competente a norma dell'art. 55 GDPR e ss.

#### **Art. 13 – Soluzioni che garantiscono la continuità lavorativa.**

Nel caso in cui un dipendente si assenti, il collega che lo sostituisce o, in sua assenza, il DSGA, potrà accedere alla casella di posta al fine di garantire la continuità lavorativa.

#### **Art. 14 – Informativa ai sensi dell'art. 13 del d. lgs. 196/2003**

L'Istituto Comprensivo "Don Bosco", in persona del Dirigente Scolastico pro-tempore, Prof.ssa Manuela Vacante è titolare del trattamento dei dati personali relativo all'utilizzo di strumenti elettronici da parte degli utenti.

**Finalità** del trattamento è la verifica del corretto utilizzo della posta elettronica e della rete Internet durante il rapporto di lavoro.

**Modalità** del trattamento dei dati è quella stabilita esclusivamente con strumenti informatici da parte di tutti gli utenti ed operatori.

**Comunicazione** dei dati. Il trattamento di verifica è effettuato con gradualità per aree aggregate per cui i dati non verranno comunicati con riferimento al singolo utente. La comunicazione, nel caso in cui si accerti un uso indebito della singola postazione sarà data al Dirigente Scolastico per la valutazione del caso sotto il profilo disciplinare.

**I diritti dell'interessato** sono garantiti in quanto lo stesso potrà farli valere invocando, come in premessa, gli artt. dal 16 al 22 facendo pervenire richiesta scritta dei diritti che vuole difendere direttamente al Dirigente Scolastico in qualità di Titolare o al responsabile del trattamento dei dati.

#### **Art. 15 – Modalità di uso personale dei PC**

Non sono previste modalità di uso personale di mezzi informatici della scuola con pagamento o fatturazione a carico persona.

La Dirigente Scolastica  
**Dott.ssa Antonina Triolo**  
*Firma autografa sostituita a mezzo stampa  
ai sensi dell'art.3, comma 2 del decreto legislativo n.39/93*

