<< Intestazione scuola >>

Disciplinare Interno per l'uso di Internet e della posta elettronica da parte del personale scolastico

1. Premessa

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si è ormai affermato come strumento per migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni.

I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più utilizzano strumenti come la posta elettronica ed Internet non solo per fornire servizi all'utenza e per migliorare la propria efficienza, ma anche per svolgere l'attività didattica. Di fatto, anche grazie alla diffusione di procedure di lavoro agile (c.d. smart working) e all'uso di servizi in cloud promosso dal Piano Triennale per l'Informatica, l'uso di piattaforme informatiche per svolgere l'attività lavorativa o didattico/formativa, anche da casa, è ormai entrato nella ordinaria attività di un istituto scolastico.

E' pertanto necessario che siano adottate adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti. A questo proposito si richiama quanto viene riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.

A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").

Con il presente disciplinare si fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

2. Principi

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del Reg. UE 679/2016 (GDPR) e del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici.

L'Istituto Scolastico garantisce che il trattamento dei dati personali dei dipendenti relativo all'utilizzo da parte degli stessi di risorse informatiche proprie o dell'amministrazione, si conforma ai seguenti principi:

a) il **principio di minimizzazione**, 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 (art. 3 del Codice; par. 5.2 del Provvedimento);

b) il **principio di trasparenza**, secondo cui le caratteristiche dei trattamenti devono essere rese note agli interessati poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori

3. Utenti autorizzati all'uso di Internet e delle dotazioni informatiche

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 3 tipologie di utenti:

1) Personale ATA: autorizzato all'uso per lo svolgimento della propria mansione lavorativa
2) Personale docente: autorizzato all'uso per qualunque attività educativa, didattica e formativa.
3) Alunni: autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti

Il presente regolamento si riferisce all'uso delle dotazioni informatiche da parte del personale scolastico.

4. Gestione delle password

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'accesso ai sistemi informatici da parte del personale amministrativo può avvenire solo a seguito della digitazione di una password personale che dovrà essere aggiornata con regolarità. A proposito della gestione delle password si danno le seguenti indicazioni:

1. conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione: le password e i dati di accesso sono personali e devono essere mantenuti riservati per garantire la sicurezza dei dati aziendali (non condividere le credenziali con i colleghi).
2. scollegarsi dal sistema ogni qualvolta ci si debba assentare dal locale nel quale è ubicata la stazione di lavoro o nel caso si ritenga di non essere in grado di presidiare l'accesso alla medesima: 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.
3. Informare immediatamente l'amministratore di sistema in caso di sospetto accesso non autorizzato in modo da evitare ulteriori problemi di sicurezza.

5. Utilizzo del personal computer

Nell'uso del personal computer messo a disposizione dall'istituto scolastico per lo svolgimento dell'attività lavorativa dovranno essere rispettate le seguenti disposizioni:

1. *Utilizzare il PC solo per scopi lavorativi e non personali:* il PC sul luogo di lavoro deve essere utilizzato esclusivamente per lo svolgimento delle attività lavorative e non per attività personali ad esse non attinenti. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. *Non utilizzare il PC per attività illegali o non etiche:* il PC non deve essere utilizzato per attività illegali o non etiche come la diffusione di materiale illegale, la distribuzione di malware o la divulgazione di informazioni riservate
3. *Mantenere aggiornato il software di sicurezza e antivirus:* è importante mantenere costantemente aggiornato il software di sicurezza e antivirus per proteggere il sistema da eventuali minacce informatiche.

4. *Salvare i dati solo su server o dispositivi di storage autorizzati:* i dati aziendali devono essere salvati solo su server o dispositivi di storage autorizzati per garantirne la sicurezza e la privacy. L'uso di dispositivi esterni non autorizzati come chiavette USB o hard disk esterni possono rappresentare una minaccia per la sicurezza dei dati aziendali, pertanto non è permesso collegare tali dispositivi senza autorizzazione.
5. *Non modificare le configurazioni del PC senza autorizzazione esplicita da parte del responsabile IT:* non modificare le impostazioni del computer, poiché ciò potrebbe causare problemi di funzionamento e compromettere la sicurezza del sistema.
6. *Spegnere il PC ogni sera o quando ci si allontana dalla postazione di lavoro:* spegnere il computer quando non si utilizza permette di ridurre il consumo di energia e previene l'accesso non autorizzato.
7. *Archiviare solo le informazioni pertinenti all'attività lavorativa, evitando l'archiviazione di informazioni personali o non pertinenti***:** archiviare solo le informazioni necessarie per svolgere le attività lavorative, poiché l'archiviazione di dati personali o non pertinenti potrebbe violare la privacy degli utenti.
8. *Non riprodurre o duplicare programmi informatici* senza autorizzazione esplicita dei proprietari del software, poiché ciò potrebbe violare il diritto d'autore e la proprietà intellettuale

6. Misure di tipo tecnologico connesse all'uso della posta elettronica

Ai fini dell'utilizzo corretto delle caselle di posta elettronica nello svolgimento dell'attività lavorativa si mettono in evidenza i seguenti punti:

1. Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione attinente all'attività lavorativa dovrà avvenire per mezzo delle caselle istituzionali
2. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure della Scuola e del Ministero della Pubblica Istruzione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale
3. E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del Ministero della Pubblica Istruzione.
4. L'accesso alle caselle di posta elettronica su sistemi di proprietà della scuola deve avvenire tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali.
5. E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali.
6. Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio contattare l'amministratore dei sistemi informatici.
7. Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
8. L'iscrizione a "mailing list" esterne è concessa solo per motivi lavorativi, prima di iscriversi occorre verificare in anticipo se il sito è affidabile. In caso di dubbio, è necessario

contattare preventivamente il DS, il DSGA o un suo delegato, che definiranno l'effettiva sicurezza della stessa, consultandosi, se necessario, con l'amministratore dei sistemi informatici.

Limitatamente alle caselle fornite agli utenti scolastici e realizzate nella piattaforma cloud adottata, l'Amministrazione registra e conserva per il tempo necessario a garantire la gestione dei sistemi e la sicurezza i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio; destinatario/i; giorno ed ora dell'invio; esito dell'invio. L'amministrazione, inoltre, potrà procedere alla cancellazione dell'account qualora l'esistenza dello stesso non sia più compatibile con le condizioni e le finalità per cui era stato originariamente attivato (ad es. il dipendente non è più in servizio, l'alunno termina la propria permanenza nell'istituto).
(VERIFICARE CON IL VOSTRO AMMINISTRATORE DI SISTEMA)

7. Misure di tipo tecnologico connesse all'uso di Internet

Nell'uso di internet sul posto di lavoro, al fine di evitare usi impropri della navigazione, dovranno essere rispettate le seguenti disposizioni:

1. Al personale non è consentito, durante le ore di lavoro:
   - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
   - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting social network similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
   - Utilizzare sistemi Social Network quali twitter, facebook, etc., salvo specifiche attività espressamente autorizzate per le attività lavorative
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'istituto si è dotato di strumenti specifici che consentono:

- La protezione da accessi non autorizzati provenienti da Internet
- Controlli antivirus centralizzati
- configurazione di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'accesso ai siti inseriti in black list individuati dall'Istituto, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato), anche in modo differenziato per le diverse postazioni o tipologie di accesso;
- la determinazione di informazioni sulla navigazione Internet che consentono la conservazione di informazioni relative ad utente, PC, ora di accesso, pagine accedute, etc.

(VERIFICARNE LA VERIDICITA' CON IL VOSTRO AMMINISTRATORE DI SISTEMA)

Si precisa che ulteriori tracce dell'operato di ciascun utente, lasciate sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per l'individuazione e la sanzione di eventuali comportamenti che violano il presente regolamento.

La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

8. Disposizioni per il lavoro da remoto (telelavoro)

Il personale che svolge la propria attività in modalità di lavoro agile deve attenersi alle raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto e riportate di seguito:

1. segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione;
2. utilizza i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows XP o windows 7 di cui Microsoft ha terminato il supporto);
3. effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo;
4. assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
5. assicurati che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale;
6. non installare software proveniente da fonti/repository non ufficiali;
7. blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro;
8. non cliccare su link o allegati contenuti in email sospette;
9. utilizza l'accesso a connessioni Wi-Fi adeguatamente protette;
10. collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione);
11. effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Nello svolgimento dell'attività lavorativa da remoto dovranno anche essere garantiti i seguenti punti:

- Utilizza esclusivamente servizi cloud certificati dall'amministrazione (tramite nomina a responsabile del trattamento) per il trattamento dei dati personali di cui l'amministrazione è titolare;
- nel caso in cui utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installa un buon antivirus e fai una accurata scansione preventiva per rimuovere qualunque software malevolo;
- non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza;
- non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali;
- accertati di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertati di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato);
- se utilizzi una connessione wi-fi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wi-fi).

9. Trattamenti esclusi

L'Istituto Scolastico non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.
L'Istituto Scolastico non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;

10. Gradualità dei controlli

1. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.
2. Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
3. La presenza di successive anomalie potrà comportare controlli su base individuale.
4. La rilevazione delle anomalie e delle verifiche tecniche è a cura dell'Amministratore di Sistema che potrà anche intervenire su richiesta del Dirigente Scolastico per la verifica di situazioni anomale o sospette.
5. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

11. Sanzioni dipendenti

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.
2. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalle leggi (art. 171-ter - art. 248/00 - art. 547 - art.594 e 595 - art. 600-ter e seg. - art. 615 ter - art. 615 quater- art. 615-quinques - art. 617 quater - art. 617 quinquies - art. 617 sexies - art. 635-bis - art. 640 e 640 ter).

12. Disposizioni ulteriori

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.
2. L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 11 del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.
3. Il presente documento viene portato a conoscenza di tutti i lavoratori, indicati all'art. 1 del presente Disciplinare, mediante pubblicazione nei sito internet.

13. Aggiornamento periodico

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.