ALLEGATO A:
ISTRUZIONI OPERATIVE PER LE PERSONE AUTORIZZATE A TRATTARE I DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679 "GENERAL DATA PROTECTION REGULATION"

Sommario

Istruzioni e regole per il trattamento di dati con l'ausilio di strumenti elettronici

Tutto il personale che partecipa ai trattamenti (Personale autorizzato al trattamento, interno ed esterno, dall'Istituto Scolastico, in persona del Dirigente, d'ora in avanti "**Titolare**") che a qualunque titolo accede al sistema informativo che si trovi all'interno della rete informatica, collegato o meno a tale rete, o che custodisce qualsiasi dato personale (anche cartaceo) di competenza del **Titolare** e non destinato alla diffusione dovranno attenersi a quanto riportato di seguito. In particolare si evidenzia che:

- L'accesso a un qualunque tipo di trattamento di dati personali con strumenti elettronici è sempre subordinato al superamento di una procedura di autenticazione informatica che prevede l'inserimento di un codice di identificazione personale (username) e di una parola chiave (password) riservata e conosciuta solamente dal medesimo utilizzatore.
- Il successivo accesso a strumenti informatici necessari per il trattamento di dati personali per una corretta esecuzione del proprio incarico è garantito dalla configurazione sul proprio profilo di ulteriori livelli di credenziali di autenticazione.
- Il personale autorizzato deve rendersi conto che la parola chiave rappresenta la prima barriera in una strategia di accesso selettivo a dati personali, e pertanto una parola chiave selezionata con criteri non soddisfacenti può portare alla compromissione dell'intera rete informativa.

Per queste ragioni ciascuno **è responsabile della segretezza della parola chiave associata al proprio codice di identificazione e tenuto a prendere tutte le iniziative appropriate per garantire la sicurezza della stessa**.

Pertanto, è indispensabile che tutto il personale prenda buona nota di quanto appresso illustrato e che si attengano strettamente a queste indicazioni.

Linee guida per la costruzione delle parole chiave

Le scelte del **Titolare** in merito alle caratteristiche delle parole chiave prevedono:
Password per l'accesso all'ambiente Windows:

- definizione della password al primo accesso dell'utente, dopo l'attivazione o riattivazione del proprio account.
- password nota SOLO all'incaricato, che ha la facoltà di cambiarla autonomamente in qualsiasi momento.
- composta da almeno 8 (otto) caratteri
- contenente caratteri di almeno tre delle seguenti categorie:
    - lettere maiuscole (da A a Z)
    - lettere minuscole (da a a z)
    - numeri (da 0 a 9)
    - caratteri non alfanumerici (ad esempio , !, $, #, %)
- non contenente riferimenti agevolmente riconducibili all'utilizzatore
- cambiamento della password ogni **6 mesi** per gli account autorizzati al trattamento di dati comuni

- cambiamento della password ogni **3 mesi** per gli account autorizzati al trattamento delle categorie particolari di dati 0
- la nuova password impostata dall'utente non potrà essere uguale a quella in scadenza ovvero alle ultime quatto (4) utilizzate

Inoltre, per gli eventuali ulteriori sistemi che prevedono l'inserimento di password, occorre attenersi, laddove possibile, alle regole sopra citate.
Si riportano alcune indicazioni per aiutare nella scelta di password che possono considerarsi sicure.

Parole chiave sicure

Sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso
- non devono essere basate su informazioni personali, come nomi di membri della famiglia, date di nascita, anagrammi o combinazione di nomi e simili
- un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze.

Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:

- creare una parola chiave, basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata - ad esempio "7000 caffè di Alex Britti" diventa "7000cffAB"
- la parola chiave può essere formata abbreviando una intera frase come ad esempio "Chi fa da se fa per 3!" diventa "Cfdsfx3!".

Attenzione: non usare mai gli esempi sopra illustrati come parola chiave

Parole chiave deboli

Si sottolinea che le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- la parola chiave si può trovare in un comune dizionario italiano, in inglese od altra lingua comune
- la parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di personaggi di fantasia
- sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili
- è da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio Giovanni1, oppure 1Giovanni.

Istruzioni e raccomandazioni per la protezione della parola chiave e la diligente custodia dei dispositivi di autenticazione in possesso ed uso esclusivo

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni e per sistemi di autenticazione esterni alla rete informatica del **Titolare**, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività non legate all'attività lavorativa.

La parola chiave prescelta non deve essere condivisa con alcun soggetto ivi inclusi i superiori, a qualsiasi livello.
Di seguito un elenco degli accorgimenti da adottare:

- non rivelate una parola chiave attraverso il telefono a chicchessia
- non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio
- non archiviate la parola chiave in chiaro in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile
- non scrivete una parola chiave in un messaggio di posta elettronica
- non rivelate la parola chiave al vostro superiore
- non parlate di parole chiave di fronte a terzi
- non date alcuna indicazione in merito al formato ed alla lunghezza della parola chiave, che utilizzate
- non svelate la parola chiave su questionari o su formulari di sicurezza
- non rivelate la parola chiave ad un vostro collega di lavoro
- non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di memorizzare la parola chiave.

Inoltre il Personale autorizzato a cui sono stati consegnati dei dispositivi per l'autenticazione (token, smart card, ecc.) sono personalmente responsabili della custodia di tali dispositivi e devono informare repentinamente un proprio superiore gerarchico nel caso di perdita o furto.
Nel caso di operazioni sistemistiche che richiedano la vostra password (es: cambio del PC o installazione di programmi), il **Tecnico informatico** la cambierà, dandovene comunicazione. Al primo utilizzo del PC è obbligatorio che modifichiate subito la password.
Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il **Tecnico informatico o il DSGA**.
Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al **Tecnico informatico** e, nel caso in cui avete il minimo sospetto di una perdita di dati, occorre informare tempestivamente il **Tecnico informatico** e il **DSGA** del Data Breach subito.
Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il **Tecnico informatico** effettui tentativi di violazione della vostra parola chiave. Nel caso il tentativo abbia esito positivo, vi verrà chiesto di sostituire immediatamente la parola chiave.
Nel caso si abbia qualsiasi dubbio afferente alle modalità sicure di generazione, utilizzo e conservazione delle parole chiave, deve rivolgersi **Tecnico informatico** per ottenere opportuni chiarimenti ed istruzioni.

Accesso ai dati ad opera del Titolare in caso di emergenza

Si informa che il **Titolare** è tenuto ad adottare idonee e preventive procedure che consentano l'accesso ai dati e ai sistemi, protetti dalla componente riservata delle credenziali (password) o da dispositivi in uso esclusivo al personale, in caso di prolungata assenza o impedimento degli stessi e in caso si renda necessario e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
Resta inteso che dal momento in cui, per l'accesso ai dati in caso di emergenza, il **Titolare** o il **Tecnico informatico** procedano al reset della password in uso esclusivo all'utente, allo stesso non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati od accessi non consentiti ai dati personali, di cui al suo profilo di autorizzazione.

Tale responsabilità verrà pienamente rimessa in essere non appena l'utente avrà avuto la possibilità di selezionare una nuova parola chiave.

Disattivazione delle credenziali di accesso

Si sottolinea che per motivi di sicurezza le credenziali di accesso assegnate saranno disattivate in caso di:

- perdita del diritto di accesso ai dati per qualunque motivo
- inutilizzo delle credenziali per un periodo superiore a 6 mesi
- accesso in caso di emergenza ad opera del **Titolare**
- ripetuti tentativi di accesso falliti (disattivazione per alcuni minuti)

Qualora ci si trovasse nella impossibilità ad accedere al sistema con le credenziali assegnate occorre rivolgersi al **Tecnico informatico**.
Nel caso di perdita del diritto di accesso, come ad esempio per cessazione del rapporto lavorativo, le credenziali assegnate saranno disattivate e la posta elettronica associata al personale autorizzato sarà re-diretta all'indirizzo di un altro soggetto per il periodo che il **Titolare** riterrà necessario, dopodiché la casella di posta sarà cancellata.
I file di lavoro saranno trasferiti ad altro soggetto interno, sia esso superiore gerarchico o responsabile di area.

Sessioni di trattamento dati incustodite

Si raccomanda di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento di dati personali, in particolare qualora sia necessario allontanarsi temporaneamente dal posto di lavoro. Si ricorda che la pressione contemporanea dei tasti Ctrl + Alt + Canc attiva la finestra di "Protezione di Windows" dalla quale è possibile premere il pulsante "Blocca computer" per bloccare la stazione di lavoro senza la necessità di uscire dai programmi in uso. Una volta ritornati davanti alla propria postazione, per riprendere l'operatività è necessario seguire le istruzioni a video delle finestre di Windows premendo nuovamente i tasti Ctrl + Alt + Canc e inserendo la propria password.
Per cautelarsi ulteriormente dalle eventualità di lasciare sessioni di trattamento di dati personali incustodite, è possibile impostare un blocco automatico della propria postazione di lavoro che richieda l'inserimento della password in fase di ripristino. Per far ciò è necessario eseguire le operazioni specifiche per ogni sistema operativo. Rivolgersi al proprio servizio IT per un supporto specifico.
Il blocco automatico con password è da considerarsi, comunque, una misura atta a ridurre, e non ad eliminare a causa del suo ritardo di attivazione, possibili rischi di trattamento dati da parte di persone non autorizzate. E' necessario, pertanto, prendere tutte le cautele affinché ciò non avvenga, ad esempio mediante il blocco della stazione di lavoro nella modalità manuale sopra identificata.

Istruzioni e raccomandazioni per l'organizzazione dei dati su File System

Si ricorda che le uniche aree autorizzate al salvataggio di dati non strutturati su file system sono gli spazi riservati sul server.
Nello specifico, sui server **di File Sharing** sono presenti delle unità logiche strutturate in sottocartelle, che sono configurate per consentire l'accesso agli aventi diritto.
Le sottocartelle sono caratterizzate come segue:

- Strutturazione delle cartelle in relazione alla tipologia di lavoro (amministrativo, paghe, personale…)
- Ogni utente può chiedere l'attivazione di una propria cartella personale, resa ad esso accessibile e, preterintenzionalmente, agli Amministratori di Sistema.
- Esiste un'area per lo scambio di dati accessibile a tutti gli utenti autenticati.

Tali spazi sono configurati al fine di garantire la sicurezza e la custodia dei dati in conformità a quanto previsto dal profilo di incarico assegnato, impedendo accessi non consentiti, assicurando disponibilità dei dati in caso di emergenza e sottoposti a backup.
Qualora un utente, accedendo al server, si accorga di:

- aver involontariamente cancellato un file
- aver involontariamente corrotto un file
- non reperire il file che si vuole aprire

è necessario che si rivolga al **Tecnico informatico**.
Nel caso non sia stato possibile il recupero dei file, il **Tecnico informatico** insieme all'autorizzato valuterà l'opportunità, in caso di sospetta perdita di dati personali, di informare il responsabile dei Data Breach.

Ogni salvataggio in locale è fortemente sconsigliato e sotto la totale responsabilità dell'incaricato.

Per chi dispone di notebook ed abbia necessità di avere in locale dei documenti, è opportuno attivare una procedura di **sincronizzazione automatica dei file,** chiedendo autorizzazione al Dirigente Scolastico e coinvolgendo il **Tecnico informatico**.
Se invece si utilizzano supporti rimovibili (cd-rom, chiavi USB…) per il trasferimento e la modifica di file, occorre mantenerne una copia aggiornata sul server della rete informatica del **Titolare**.

Istruzioni e raccomandazioni per la custodia, uso e distruzione di supporti rimovibili

In linea generale, non è permessa la copia su supporti rimovibili (cd/dvd, chiavette USB, hard disk, ecc.) di dati personali, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.
Ciò premesso, ove nello svolgimento della normale attività assegnata, nell'ambito del profilo di autorizzazione, sia indispensabile effettuare una copia di dati personali su supporti rimovibili, occorre attenersi alle seguenti cautele:

- utilizzare solo ed esclusivamente supporti forniti dal Titolare e con l'autorizzazione del proprio superiore gerarchico o del Tecnico informatico.
- accertarsi che il supporto rimovibile sia debitamente formattato e privo di altri file, che potrebbero essere infettati da virus a contenere dati di natura diversa. Nel dubbio, è sempre bene provvedere alla formattazione *ex novo* del supporto, prima di registrare dati personali
- ove possibile, i dati devono essere protetti da un sistema di cifratura
- qualsiasi supporto rimovibile deve essere contrassegnato da un'etichetta, con una indicazione in chiaro od in codice, tale da permettere di riconoscere immediatamente il contenuto del supporto in questione, ed evitare che si possa confondere con altri supporti e facilitare la procedura di identificazione del supporto smarrito per l'eventuale segnalazione del Data Breach.
- I supporti rimovibili contenenti dati personali devono essere sempre direttamente e personalmente custoditi da chi ha realizzato la copia.

Qualora i dati contenuti su supporti rimovibili non abbiano più ragione di essere, si deve provvedere immediatamente alla formattazione dei supporti.
Poiché i supporti rimovibili potrebbero essere danneggiati da campi magnetici, per evitare la perdita anche

accidentale dei dati, tali supporti non devono mai essere avvicinati ad un campo magnetico, come ad esempio il magnete di un altoparlante, oppure i trasformatori utilizzati nelle lampade da tavolo.
Si faccia sempre attenzione a non dimenticare il supporto rimovibile all'interno del computer, quando lo si spegne o ci si allontana.
Il supporto rimovibile contenente dati personali non deve mai essere lasciato incustodito, ma deve essere posto all'interno di una custodia sicura. In funzione della criticità dei dati archiviati e quindi del contenuto di eventuali dati sensibili, può essere considerato sicuro un cassetto della scrivania chiuso a chiave, un armadio, una cassaforte, o un altro contenitore idoneo alla custodia di tali supporti.
Se il supporto viene smarrito o rubato occorre immediatamente avviare la procedura di rilevazione del Data Breach.

Istruzioni e raccomandazioni per l'utilizzo di hardware e software

Il software installato in ciascuna macchina (sistema operativo, Office Automation…) nonché le relative configurazione hardware, rispecchiano la condizione necessaria e sufficiente per il consueto lavoro da svolgersi e comunque valutato e stabilito dal **Titolare**.
Qualora riteniate necessario disporre di un nuovo software o di un aggiornamento hardware per le consuete mansioni, è proibito procedere all'auto-installazione dei medesimi ma è necessario informare il **Tecnico informatico** che valuterà l'opportunità dell'upgrade della macchina.
È bene ricordare che ogni software ha una licenza e l'uso improprio di questa può portare a conseguenze civili.
Inoltre agli utenti dei Personal Computer non è consentito l'accesso ai parametri di configurazione dei software e del Sistema Operativo, per modificare i quali è sempre necessaria una specifica attività da parte del **Tecnico informatico**.

Istruzioni e raccomandazioni per l'utilizzo di internet e del servizio e-mail

L'utilizzo di internet e della posta elettronica, sono resi disponibili dal **Titolare** per scopi lavorativi, cioè al fine di ottemperare alle mansioni previste dal proprio ruolo.
Il servizio e-mail è considerato uno strumento di lavoro a tutti gli effetti, come il fax, il telefono e pertanto l'Incaricato deve farne un uso appropriato, che non esuli dal contesto lavorativo in cui opera.
È necessario ricordare che l'utilizzo dell'e-mail può comportare dei rischi derivanti dalla possibile intercettazione della medesima e, quindi, i documenti in essa contenuti potrebbero essere letti e/o utilizzati da persone non autorizzate al trattamento (per tale motivo è vietato inviare a mezzo mail file contenenti categorie particolari di dati, come ad esempio dati sanitari). Per l'invio di file o documenti contenenti categorie particolari di dati è consigliabile l'utilizzo di PEC o file con password (da comunicare al destinatario attraverso altro canale e non nello stesso messaggio di posta elettronica).
Nel momento in cui una e-mail viene stampata, assume tutti le caratteristiche di un documento cartaceo e il personale deve attenersi alle istruzioni in merito a questa tipologia di trattamento.
È necessario, inoltre, prestare molta attenzione alle e-mail che giungono nella propria casella di posta, in quanto queste potrebbero essere state inviate in automatico da sistemi infetti da virus e quindi potrebbero contenere esse stesse dei virus. Qualora giungessero e-mail da mittenti sconosciuti evitare, in prima analisi, di aprire eventuali allegati.
Importante ricordare che, nei casi di inoltro di e-mail a più destinatari esterni al **Titolare** che non hanno l'esigenza di conoscere gli altri destinatari, occorre utilizzare la funzionalità di invio per conoscenza nascosta (Ccn).

Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di phishing

Il phishing è un'azione volta al furto dell'identità informatica, cioè di quelle informazioni, generalmente riservate, che permettono di identificare un soggetto che accede ad un sistema informatico (es. le

credenziali di accesso al pc, le credenziali di accesso al portale internet del conto corrente bancario, ecc.).
Il phishing inizia con la ricezione di una e-mail inviata dal truffatore alle potenziali vittime. Di norma il messaggio di posta ha un aspetto formale e cerca di indurre il destinatario ad effettuare una serie di operazioni abbastanza usuali per coloro che usufruiscono dei servizi web on-line.
Ad esempio l'invito a "cliccare" sull'indirizzo del sito (in questo caso pirata) e la presentazione di una pagina web che appare con tutte le caratteristiche dell'azienda con la quale l'utente ha stipulato il servizio on-line.
Se la vittima inserisce i propri dati tramite l'apposita pagina web, scatta il meccanismo di raccolta delle informazioni che, una volta in possesso del truffatore, possono essere usate in modo fraudolento.
Si riporta un esempio di e-mail phishing.
"*Gentile Cliente,*
questa e-mail Le è stata inviata dai server di (di solito il nome di una banca) per evitare che il suo account (nome utente e password) sia disattivato per inutilizzo. Per completare l'operazione è sufficiente che Lei faccia click sul link seguente ed effettui il log-in come di consueto. Tutto questo per garantire la protezione dei suoi dati. Infatti è stato riscontrato che molti utenti non effettuano l'accesso da tanto tempo. Per verificare il suo account faccia click sul link seguente e, quindi, effettui il log-in come di consueto:
www.nomebanca.com/verificaaccount "
Per scongiurare le minacce di phishing è utile attenersi ai seguenti punti:

- evitare di rispondere a richieste di informazioni personali ricevute tramite posta elettronica, se non si ha certezza della provenienza. Nel dubbio, è sempre preferibile verificare l'attendibilità dell'informazione o della richiesta contattando il mittente con canali diversi (es. telefono).
- anche se il link nella e-mail o la barra degli indirizzi web risulta (apparentemente) corretto, è bene sapere che esistono delle tecniche, usate dagli hacker, per mascherare l'indirizzo fasullo con uno corretto. Se c'è il minimo sospetto è meglio evitare di "cliccare" sui link per accedere ai relativi siti web. Questi collegamenti potrebbero condurre al sito pirata. Invece, aprire una nuova finestra del browser e digitare a mano l'indirizzo.
- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza dell'icona del lucchetto sulla parte in basso a destra del browser. Fare doppio click sul lucchetto per verificare il certificato SSL.

In ogni caso è opportuno notificare al **Tecnico informatico** eventuali sospetti di phishing, furto d'identità o usi illeciti delle proprie informazioni e, nel caso ci fosse il fondato sospetto di una violazione dei dati personali, occorre informare i referenti delle procedura sui Data Breach.

Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di pharming

Il pharming è un'estensione estremamente sofisticata del phishing. A differenza di quest'ultimo, gli attacchi di Pharming rimangono nascosti in un computer connesso alla rete e raccolgono informazioni sui dati finanziari durante la normale navigazione delle vittime. Gli utenti che vogliono collegarsi a un sito web sono, a loro insaputa, dirottati verso un sito artefatto simile a quello originale. Una volta impiantato lo schema di pharming, può partire l'attività dannosa contro un gran numero di siti che l'utente visita regolarmente, senza che la vittima se ne renda minimamente conto.
Per identificare le minacce di pharming è utile sapere che:

- i processi di login, verifica o informazione mostrati nei siti pirata non sono esattamente identici a quelli del sito autentico
- è probabile che i siti di pharming richiedano informazioni di verifica o personali che solitamente non sono necessarie

- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza dell'icona del lucchetto sulla parte in basso a destra del browser. Fare doppio click sul lucchetto per verificare il certificato SSL
- in un sito sicuro, l'indirizzo (URL) che compare nel browser dovrebbe contenere il prefisso https:// nella barra dell'indirizzo. I siti di pharming generalmente non hanno certificati SSL per cui il prefisso http:// rimane anche quando si devono inserire dati riservati
- se il browser rileva l'esistenza di un problema con il certificato SSL, invece di ignorarlo, gli utenti devono cogliere l'occasione per controllare il certificato e considerarlo come un segno evidente di sito fraudolento.

In ogni caso è opportuno notificare al **Tecnico informatico** eventuali sospetti di pharming e, nel caso ci fosse il fondato sospetto di una violazione dei dati personali, occorre i referenti delle procedura sui Data Breach.

Istruzioni per il trattamento di dati senza l'ausilio di strumenti elettronici

Gestione quotidiana pratiche

Istruzioni per i dati personali in genere

- Le pratiche contenenti dati personali (di seguito: "le pratiche") devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave.
- Le pratiche devono essere prelevate, a cura degli utilizzatori, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali – ed in ogni caso al termine della giornata lavorativa – devono essere riposte negli archivi. Ciascun utilizzatore deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non incaricati del trattamento (aree di passaggio, sale d'attesa, sale riunioni, ecc.).
- Anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche devono essere riposte negli archivi, salvo adeguata garanzia di controllo da parte di altri utilizzatori autorizzati ai medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite.
- Lo smarrimento o il furto di informazioni devono essere comunicati immediatamente ai referenti delle procedura sui Data Breach.
- È buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Le stampe e le fotocopie inutili devono essere distrutte nell'apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli.

Istruzioni per le categorie particolari di dati e per i dati relativi a condanne penali o reati

Oltre a quanto previsto per i dati personali in genere, le pratiche contenenti categorie particolari di dati e dati relativi a condanne penali o reati devono essere conservate in archivi ad accesso controllato, devono essere controllate e custodite fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altri utilizzatori che non siano autorizzati ad accedere alle informazioni

sensibili), e devono essere restituite al termine delle operazioni affidate.
Quando circolano all'interno dell'Istituto scolastico devono essere inserite in busta chiusa; stesso discorso qualora vi fosse la necessità di comunicare tali dati e documenti ad altri Enti (es. Comuni o ASL) autorizzati in forza di norma di legge o regolamento a riceverli.
Compete agli utilizzatori il controllo della chiusura a chiave degli armadi contenenti tale tipologia di dati e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo. **I documenti contenenti dati ultra-sensibili (es. stato di salute relativo ai BES o DSA devono essere custoditi in cassaforte).**

Gestione chiavi

I soggetti chiamati a gestire le chiavi "fisiche" degli archivi devono:

- all'atto della consegna delle chiavi, verificarne subito il corretto funzionamento;
- verificare che le chiavi non restino inserite negli armadi/archivi;
- conservare le chiavi in un luogo e con modalità che ne garantiscano una sicurezza adeguata anche al tipo di archivio;
- non metterle a disposizione né mostrarle ad estranei;
- in caso di smarrimento o sottrazione, farne immediata segnalazione ai referenti delle procedura sui Data Breach e richiedere la sollecita sostituzione della serratura, spostando se del caso, per il tempo necessario, i documenti dall'archivio non protetto.

Compete a tali soggetti il controllo della chiusura a chiave degli armadi contenenti dati sensibili e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo.

Scarti di archivio

Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere trattate da soggetti non incaricati/autorizzati.
In particolare i documenti contenenti categorie particolari si dati devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione, ove disponibili, altrimenti vanno ridotti in piccoli pezzi.

Consegna di certificazioni medico-sanitarie a mezzo di altri soggetti

La consegna di certificazioni mediche, o comunque di altre informazioni personali delicate relative ai dipendenti o a terzi può essere effettuata anche tramite altri dipendenti o comunque altre persone a condizione che:

- la documentazione sia di regola consegnata in busta chiusa;
- prima della consegna, la documentazione non sia lasciata incustodita. Di regola, ove non sia presente il destinatario, la documentazione va consegnata a un responsabile d'area o superiore gerarchico;
- la consegna avvenga nel minor tempo possibile.

Uso del fax e di Scanner Digitali

Non inviare FAX contenenti dati personali ad un destinatario generico (ad es. un ufficio).
Se occorre inviare un FAX contenente dati personali ad una persona autorizzata a visionarli, è opportuno

invitare la persona destinataria ad essere vicina al fax al momento della spedizione.
Riguardo ai FAX ed alle fotocopiatrici digitali con scanner di rete, il loro utilizzo è consentito per l'invio delle scansioni tramite e-mail o, se previsto nelle specifiche sedi, via rete o FTP ad una cartella di rete accessibile a tutti gli incaricati.
E necessario adottare le seguenti cautele:

- le scansioni contenenti categorie particolari di dati personali devono avvenire esclusivamente via e-mail.
- le scansioni inviate via FTP devono essere cancellate immediatamente dopo la scansione ed il successivo salvataggio da parte dell'incaricato che l'ha effettuate.
- in ogni caso è prevista la cancellazione automatica di tali aree ogni venerdì sera.

Telefonate e colloqui

Informazioni telefoniche
Il personale deve considerare che il colloquio telefonico non è, di norma, metodo adeguato per l'identificazione sicura dell'interlocutore.
Deve essere pertanto rispettata la seguente regola generale: non è consentito fornire informazioni personali telefonicamente, in quanto non è di norma possibile identificare con certezza la persona con la quale è in corso il colloquio.
La regola generale può trovare eccezioni tutte le volte in cui si possa ragionevolmente ritenere di avere sufficienti elementi per l'identificazione certa dell'interlocutore (ad esempio, in quanto esiste con l'interlocutore una consuetudine di rapporto, tale da garantire di fatto il riconoscimento; oppure in forza di una verifica su alcuni dati personali –data di nascita, codice fiscale, ecc.; e così via).
Comportamento nel corso delle telefonate
Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, anche utilizzando cellulari, per evitare che dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Misure di controllo e verifica

Al fine di forzare, monitorare e verificare l'adozione delle misure di sicurezza, il **Titolare**, relativamente agli strumenti elettronici di trattamento dati, adotta i seguenti accorgimenti tecnici:

- ai nuovi utenti sarà obbligatoriamente richiesta la scelta di una password personale al primo accesso al sistema
- non saranno accettate dal sistema password di lunghezza inferiore a 8 caratteri
- saranno accettate dal sistema solo password contenenti caratteri di almeno tre delle seguenti categorie:
    - lettere maiuscole (da A a Z)
    - lettere minuscole (da a a z)
    - numeri (da 0 a 9)
    - caratteri non alfanumerici (ad esempio , !, $, #, %)
- il sistema ricorderà agli utenti l'avvicinarsi della scadenza della propria password e imporrà il cambio della stessa allo scadere, impostato almeno ogni 3 mesi per gli account autorizzati al trattamento di dati sensibili, ogni 6 mesi per gli altri.
- Ove possibile il sistema verificherà che la nuova password inserita sia differente dalle ultime 4 utilizzate.

Inoltre il **Titolare** effettuerà, periodicamente, specifiche verifiche al fine di valutare se gli strumenti elettronici affidati sono usati in attinenza all'ambito lavorativo e secondo le istruzioni impartite.
Relativamente al trattamento di dati senza l'ausilio di strumenti elettronici, il **Titolare** effettuerà, periodicamente, specifiche verifiche al fine di valutare se sono seguite le procedure e le istruzioni impartite.

Istruzioni specifiche per Assistenti Amministrativi

Tutto il personale ATA che tratta, o si trova a trattare, in qualunque modo, dati personali del **Titolare** deve attenersi alle seguenti procedure:

- agire in modo lecito e corretto secondo le prescrizioni e nel rispetto dei principi previsti dal Regolamento UE 2016/679 e del D. Lgs. 196/2003 (e s.m.i.) con particolare riferimento alle comunicazioni, anche elettroniche, alla ricezione, alla consegna, al trasporto e alla duplicazione di documenti contenenti dati personali;
- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- non utilizzare i dati personali trattati per finalità incompatibili con la funzione svolta;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (floppy disk, cd, dvd, pendrive, ecc.) che contengono dati personali e categorie particolari di dati personali di cui all'art.9 del Regolamento Ue 2016/679 e dei dati personali relativi a condanne penali e reati di cui all'art.10 del Regolamento Ue 2016/679;
- non portare all'esterno della scuola documenti contenenti dati personali senza previa autorizzazione del Responsabile o del Titolare del trattamento;
- trattare i dati personali mediante l'utilizzo di apparecchiature in possesso dell'Istituzione scolastica;
- non memorizzare dati personali su dispositivi dell'Istituto o apparecchiature personali;
- non memorizzare password (tramite la funzione "remember password") su dispositivi dell'Istituto o apparecchiature personali;
- non pubblicare on line (nemmeno attraverso i canali social privati) circolari, dati o documenti contenenti i nomi degli studenti portatori di handicap;
- trattare i dati sulle origini razziali ed etniche solo per favorire l'integrazione degli alunni stranieri;
- utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- trattare i dati idonei a rivelare lo stato di salute per l'adozione di specifiche misure di sostegno per gli alunni disabili o con disturbi di apprendimento, per le seguenti finalità: gestione delle assenze per malattia, insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie, partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione;
- trattare i dati relativi a opinioni politiche esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza (ad esempio, le consulte e le associazioni degli studenti e dei genitori);
- prestare attenzione a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa (ad esempio i professori che devono predisporre il piano didattico personalizzato).

Istruzioni specifiche per Docenti

Tutto il personale docente che tratta, o si trova a trattare, in qualunque modo, dati personali del **Titolare** deve attenersi alle seguenti procedure:

- agire in modo lecito e corretto secondo le prescrizioni e nel rispetto dei principi previsti dal Regolamento UE 2016/679 e del D. Lgs. 196/2003 (e s.m.i.) con particolare riferimento alle comunicazioni, anche elettroniche, alla ricezione, alla consegna, al trasporto e alla duplicazione di documenti contenenti dati personali;
- accedere solo ai dati strettamente necessari all'esercizio della propria funzione;
- rispettare il divieto di diffusione e comunicazione dei dati personali salvo i casi strettamente funzionali allo svolgimento dei compiti affidati e comunque previa autorizzazione del Dirigente Scolastico;

- mantenere il riserbo sulle informazioni di cui sia venuto a conoscenza nell'esercizio della sua funzione, anche dopo la cessazione dell'incarico, senza limiti temporali;
- tutte le informazioni di cui il docente viene a conoscenza con comunicazioni, da parte di colleghi, del Dirigente, dagli assistenti amministrativi, dagli alunni e dalle famiglie, anche attraverso elaborati scritti, relative a dati personali devono essere utilizzate solo per il perseguimento dei fini istituzionali della scuola, nell'ambito della sfera d'azione professionale del docente;
- consegnare il registro di classe al collaboratore scolastico incaricato, al termine delle attività didattiche giornaliere, per la sua custodia in apposito armadio dotato di serratura nella stanza individuata come sala professori dell'edificio;
- provvedere alla tempestiva riconsegna della documentazione consultata per causa di lavoro a chi è incaricato alla sua conservazione permanente;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Dirigente o il DSGA di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi, nonché qualora si verificasse la necessità di porre in essere operazioni per finalità o modalità diverse da quelle risultanti dalle istruzioni ricevute;
- comunicare al Dirigente eventuali alterazioni di registri e/o dati personali riguardanti gli alunni;
- non portare all'esterno della scuola o effettuare copie di documenti contenenti dati personali senza previa autorizzazione del responsabile o titolare;
- non memorizzare dati personali su dispositivi dell'Istituto o apparecchiature personali;
- non memorizzare password (tramite la funzione "remember password") su dispositivi dell'Istituto o apparecchiature personali;
- svuotare il cestino ogni volta che si eliminano documenti contenenti dati personali;
- non pubblicare sui social network foto e video degli alunni e non utilizzare strumenti social (es. whatsapp e similari) per comunicare dati personali riferiti a minori;
- non pubblicare on line (nemmeno attraverso i canali social privati) circolari, dati o documenti contenenti i nomi degli studenti portatori di handicap;
- trattare i dati sulle origini razziali ed etniche solo per favorire l'integrazione degli alunni stranieri;
- utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- trattare i dati idonei a rivelare lo stato di salute per l'adozione di specifiche misure di sostegno per gli alunni disabili o con disturbi di apprendimento, per le seguenti finalità: gestione delle assenze per malattia, insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie, partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione;
- trattare i dati relativi a opinioni politiche esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza (ad esempio, le consulte e le associazioni degli studenti e dei genitori);
- prestare attenzione a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa (ad esempio i professori che devono predisporre il piano didattico personalizzato).

Istruzioni specifiche per Collaboratori scolastici

Tutti i Collaboratori scolastici che trattano, o si trova a trattare, in qualunque modo, dati personali del **Titolare** deve attenersi alle seguenti procedure:

- agire in modo lecito e corretto secondo le prescrizioni e nel rispetto dei principi previsti dal Regolamento UE 2016/679 e del D. Lgs. 196/2003 (e s.m.i.) con particolare riferimento alle

comunicazioni, anche elettroniche, alla ricezione, alla consegna, al trasporto e alla duplicazione di documenti contenenti dati personali;

- accedere solo ai dati strettamente necessari all'esercizio della propria funzione;
- rispettare il divieto di diffusione e comunicazione dei dati personali salvo i casi strettamente funzionali allo svolgimento dei compiti affidati e comunque previa autorizzazione del Dirigente Scolastico;
- rispettare, altresì, il riserbo delle informazioni di cui sia venuto a conoscenza nell'esercizio delle sue funzioni, anche dopo la cessazione dell'incarico, senza limiti temporali;
- effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- trattare i dati personali mediante l'utilizzo di apparecchiature in possesso dell'Istituzione scolastica;
- non memorizzare dati personali su dispositivi dell'Istituto o apparecchiature personali;
- non memorizzare password su dispositivi dell'Istituto o apparecchiature personali;
- non portare all'esterno dell'istituto documenti contenenti dati personali senza previa autorizzazione del Dirigente scolastico o del DSGA;
- accertarsi che al termine delle lezioni non restino incustoditi documenti contenenti dati personali e categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati, di alunni o dei docenti (quali registri di classe, registri personali dei docenti, certificati medici esibiti dagli alunni a giustificazione delle assenze), segnalando tempestivamente l'eventuale presenza al Dirigente scolastico o al DSGA e provvedendo temporaneamente alla loro custodia;
- non lasciare incustoditi e a disposizione di estranei fotocopie, documenti o altri supporti anche informatici che contengono dati personali e categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati;
- accertarsi della distruzione di documenti o supporti inutilizzati contenenti dati personali e categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati;
- segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia;
- non abbandonare la postazione di lavoro, per pausa o altro motivo, senza aver provveduto a custodire in luogo sicuro i documenti trattati;
- non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e non annotarne il contenuto nei fogli di lavoro;
- non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali e categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati;
- accertarsi dell'identità di terzi e della loro autorizzazione al ritiro della documentazione in uscita;
- provvedere alla riconsegna della documentazione consultata per causa di lavoro a chi è incaricato della conservazione permanente;
- accertarsi che al termine delle lezioni tutti i computer siano spenti e che non siano stati lasciati incustoditi materiali, in caso contrario provvedere temporaneamente alla loro custodia e segnalare la situazione tempestivamente al DSGA;
- verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al DSGA;
- procedere alla chiusura dei locali non utilizzati in caso di assenza del personale;
- procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate e le chiavi delle stanze depositate negli appositi contenitori;
- eventuali credenziali di autenticazione devono essere custodite con cura e diligenza, non possono essere messe a disposizione né rivelate a terzi, in caso di loro smarrimento è necessario dare immediata notizia al DSGA.

Istruzioni da seguire in caso di Data Breach

Nel caso in cui vi sia il fondato sospetto che si sia verificata una violazione di dati, come ad esempio:

- Perdita di documenti o fascicoli
- Distruzione archivi
- Furto o smarrimento di strumenti elettronici contenenti dati personali
- Sospetto di accesso non autorizzato nei locali deputati all'archiviazione
- Sospetto di accesso non autorizzato nella sala CED/Server
- Sospetto di accesso non autorizzato nel proprio PC
- Comportamento anomalo del proprio PC o dispositivo informatico
- Etc.…

Occorre informare tempestivamente i referenti delle procedura sui Data Breach, comunicandogli il maggior numero di dettagli circa la violazione subita:

- Data in cui è avvenuto l'evento o in cui si è venuti a conoscenza
- Modalità di esposizione al rischio, ad es.:
  - Lettura dei dati personali
  - Copia dei dati personali
  - Alterazioni dei dati personali
  - Cancellazione dei dati personali
  - Furto dei dati personali
- Dati personali oggetto della violazione (dati dei dipendenti, dei clienti, etc.)

Sanzioni

Un Incaricato che abbia violato le linee guida di sicurezza riportate nel presente documento potrebbe essere sottoposto ad azioni disciplinari, per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza relativa alla protezione dei dati personali.