POLICY INTERNA PER LA PROTEZIONE DEI DATI

v18po7

ICS Elsa Morante MIIC80900T

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA I° GRADO

Direzione – Segreteria: Via Heine, 2 - 20141 – Milano

INDICE

1. DESTINATARI 3
1.1. PRINCIPI 3
2. POLICY USO STRUMENTI ELETTRONICI 4
3. POLICY USO STRUMENTI CARTACEI 17
4. POLICY GESTIONE CHIAVI (EDIFICIO, ARCHIVI, UFFICI,..)18
5. POLICY GESTIONE ALLARMI 18
6. POLICY FOTO E VIDEO 18
7. POLICY PERSONALE COLLABORATORE 19
7.1. REGISTRO VISITATORI 19
8. POLICY PERSONALE DOCENTE 19
9. POLICY RESTORE E DISASTER RECOVERY 20
10. POLICY DATA BREACH 21
11. POLICY TRASMISSIONE DATI 23
12. POLICY SULL'ESERCIZIO DEI DIRITTI 24
13. POLICY WISTEBLOWING 25
14. DISPOSIZIONI FINALI 30

Il "titolare" del trattamento è:

ICS Elsa Morante MIIC80900T Direzione – Segreteria: Via Heine, 2 - 20141 - Milano CF 80128250158 Tel. 02.88441479 – Fax 02.88441485 Email: MIIC80900T@istruzione.it SITO WEB: www.icselsamorante.edu.it

1. DESTINATARI

Il presente documento è stato disposto in applicazione del reg. UE 679/2016 ed in particolare con lo scopo di adempiere l'obbligo di informazione sui rischi legati alla protezione dei dati. Il regolamento è suddiviso in capitoli che dovranno essere integralmente rispettati da chiunque si trovi ad operare nel contesto lavorativo.
Le prescrizioni di cui al presente regolamento si applicano in particolare secondo la seguente tabella:

CAPITOLO	PERSONALE AMMINISTRATIVO	COLLABORATORI SCOLASTICI	DOCENTI E PERS. TECNICO
Uso strumenti elettronici	x	x	x
Uso strumenti cartacei	x	x	x
Gestione chiavi	x	x	X
Gestione allarmi		x	X
Gestione foto e video	x	x	x
Personale collaboratore		X	
Personale docente			X
Disaster ricovery	x	x	X
Data Breach	x	x	X
Trasmissione dati	x	x	X
Esercizio diritti	x	x	X
Wisteblowing	x	x	X
Disposizioni finali	x	x	x

1.1. PRINCIPI

I principi che sono a fondamento della presente policy sono i medesimi espressi nel Regolamento Europeo 679/2016, ovvero:

- Principio di necessità per il quale l'utilizzo dei dati personali, attraverso l'impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite;
- Principio di correttezza secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;
- Principio di pertinenza e non eccedenza per il quale i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime.

È garantito al singolo lavoratore il diritto di accesso ai dati personali che lo riguardano con le modalità previste dalle disposizioni normative e regolamentari vigenti in materia.

Si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;

Si rimanda ai seguenti documenti rilasciati dal Garante e relativi al contesto scolastico, che si ritengono parte integrante del presente documento:

- Vademecum _La scuola a prova di privacy_ pagina doppia (anno 2016)

- La privacy a scuola - Vademecum

In considerazione di quanto disposto dal Regolamento, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Titolare del trattamento dei dati di dati oggetto del trattamento: Non è consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere, diffondere senza l'autorizzazione del Titolare del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Titolare del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

2. POLICY USO STRUMENTI ELETTRONICI

2.1. CREDENZIALI DI AUTENTICAZIONE (PASSWORD)

In ciascun dispositivo deve essere impostata una parola chiave, che deve essere selezionata con criteri di sicurezza ed aggiornata periodicamente (i vari sistemi obbligano a tale aggiornamento); ciascun addetto è tenuto a segnalare se qualche dispositivo non effettua tale procedimento

Le password di ingresso alla rete, ai programmi ed alle risorse condivise sono personali e segrete. La scelta delle password da parte dell'utente deve essere ponderata in quanto un utilizzo improprio della stessa è il modo più facile per un accesso illecito da parte di terzi alla rete e/o all'applicazione, e di conseguenza ai dati in essi custoditi a tutti gli effetti risultando con l'identità di un altro utente.

Nella gestione delle password (a qualsiasi apparecchio o strumento facciano riferimento) è necessario osservare le seguenti indicazioni:

- Modificare prontamente la password assegnata dal amministratore di sistema;
- Non comunicare ad alcuno le proprie password.
- Ricordare che nessuno è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto;
- Non scrivere/custodire le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione/strumentazione di lavoro utilizzata (no sul monitor, sotto la tastiera, sul tavolo, nel calendario, sull'agenda, nel cassetto; non creare fogli excel contenenti l'elenco delle password, nemmeno se protetti essi stessi da password)
- Non scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Non utilizzare nemmeno parole del dizionario in senso inverso;
- Non usare parole che possano essere facilmente riconducibili all'identità dell'utente come, ad esempio, il codice fiscale, il nome del coniuge o dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della via in cui si abita, il proprio numero di matricola o addirittura la stessa ID…etc;
- Non usare come password parole ottenute da una combinazione di tasti vicini alla tastiera o sequenze di caratteri;

- Non usare la stessa password per l'accesso a sistemi ed applicativi differenti;
- Non comunicare password vecchie e non più in uso quando potrebbe essere possibile ricavare da questi dati regole empiriche o personali che l'utente utilizza per generare le proprie password;
- Cambiare le password, almeno ogni sei mesi, e comunque dentro i limiti previsti dalle misure minime di sicurezza;
- Le password di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo utente, almeno ogni tre mesi;
- Creare una password di minimo otto (consigliati 10) caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati: ! $? # = * + - . , ; :
- Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera
- Non utilizzare le stesse password per più account.
- Non usare una password già utilizzata in un esempio di come si sceglie una buona password.
- Non usare parole o acronimi che si possono trovare nel dizionario.
- Non usare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234).
- Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.
- Non usare ripetizioni di caratteri (aa11).
- non deve essere uguale ad una delle ultime 5 già utilizzate.

È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
le credenziali di autenticazione non utilizzate per più di 90 giorni, saranno disattivate
L'utente è tenuto a scollegarsi dal sistema o a bloccarlo con la password di uno screen Saver (comunque ad attivazione automatica), ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima; lasciare un apparecchio incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In difetto il comportamento dell'utente si configura come negligente, inescusabile e gravemente colposo.
Non è consentito l'uso della password di accensione (BIOS)
Se fosse necessario il reset password sarà interpellato l'amministratore di sistema che vi provvederà, tuttavia la password provvisoria assegnata, dovrà essere cambiata al primo accesso

2.2. APPARECCHI ELETTRONICI (portatili, pc desktop, tablet, spmartphone, fotocamere, …)

E' riconosciuto al titolare del trattamento il potere di svolgere attività di monitoraggio, con i mezzi ritenuti idonei allo scopo.
La regolamentazione della materia indicata, ai sensi dell'art.4, comma 1, della L.300/70, non è finalizzata ad un controllo a distanza dei lavoratori da parte del titolare, ma solo a permettere a quest'ultima di utilizzare sistemi informativi per far fronte ad esigenze produttive ed organizzative, nonché per esigenze di sicurezza nel trattamento dei dati personali

Tutte le attrezzature destinate alla raccolta, trattamento e conservazione (compresi trasmissione e ricezione) di dati sono censite, racchiuse in siti protetti e di essi è nota la ubicazione, è quindi vietato modificarne l'ubicazione, o la configurazione (anche con l'installazione di ulteriori hardware) salvo esplicita deroga da parte del titolare del trattamento
Si ricorda che i dati relativi all'accesso (log) alla postazione informatica sono registrati e conservati per un periodo di 6 mesi, dopo di che vengono automaticamente cancellati.
Tali dati saranno trattati in via del tutto eccezionale per:

- Richieste da parte delle autorità giudiziarie
- Motivate richieste dell'utente interessato
- Particolari esigenze di sicurezza

In questa ipotesi i dati saranno trattati per il tempo strettamente necessario e legato alla causa che ne ha comportato la proroga nel trattamento
A termine giornata o turno, ciascun apparecchio dovrà essere spento
Per ogni incaricato, o classi omogenee di incaricati, viene costruito un profilo di autorizzazione, che limiti l'accesso ai soli dati, rilevanti per l'attività di trattamento svolta dall'incaricato, è fatto divieto tentare di accedere a dati ulteriori. Analogamente vengono stabiliti i livelli di privilegio (privilegio di creazione, lettura, modifica, cancellazione) per ciascun incaricato è fatto divieto di manomettere o alterare il funzionamento dei software installati sugli apparecchi elettronici (antivirus, sistemi operativi, software,..)nell'uso di apparecchi elettronici si ricorda di effettuare periodicamente una copia di rispetto dei dati
È vietata l'installazione di applicativi e software ulteriori rispetto a quelli forniti dall'azienda
È vietato il riutilizzo (compresa la cessione/prestito,…) di una apparecchiatura senza prima averne eliminato i dati ivi contenuti (la sola cancellazione o formattazione non è sufficiente)
L'uso degli strumenti informatici e telematici dell'azienda è consentito solo per fini attinenti all'attività lavorativa e con le modalità conformi al presente codice di condotta.
Si ricorda che unicamente gli amministratori di sistema sono autorizzati a compiere interventi sul sistema informatico e manutenzioni sul sistema hardware.
Con cadenza semestrale gli incaricati di primo livello eseguono in maniera casuale (procedendo ad esempio per estrazione) al controllo dei LOG di almeno il 10% dei PC utilizzati dal personale amministrativo e/o su cui sono trattati dati personali in maniera sistematica; in particolare si ricercano i seguenti LOG:

4625: Login: Tentativo fallito
4723: Login: Tentativo cambio password
4724: Login: Reset password
4738: Login: Cambio password
4740: Login: Utente Bloccato
4767: Login: Utente Sbloccato

Per verificare, ad esempio, se vi siano stati tentativi anomali di accesso alle postazioni

2.3. CELLULARE:

È d'obbligo per l'utente di informare l'altro utente quando, nel corso della conversazione, è consentito l'ascolto della conversazione stessa da parte di altri soggetti (vivavoce)
Non è consentita la registrazione delle chiamate
È obbligatorio l'uso del PIN di sicurezza della sim.

L'assegnatario del dispositivo di comunicazione mobile è responsabile del suo corretto utilizzo, dal momento della presa in consegna fino alla restituzione e/o revoca, e deve porre ogni cura nella sua conservazione, per evitare danni, smarrimenti e/o sottrazioni.
In caso di furto o smarrimento dell'apparecchio, l'assegnatario deve presentare la formale denuncia di furto o smarrimento presso le competenti autorità di Pubblica Sicurezza e farne pervenire copia al titolare del trattamento
I telefoni cellulari possono essere utilizzati soltanto per ragioni di servizio.
Gli assegnatari devono comunque utilizzare il telefono cellulare nei soli casi di effettiva necessità, ponendo la massima attenzione al contenimento della spesa.
In caso di malfunzionamento o di guasto dell'apparecchio o della sim, il dipendente deve rivolgersi al Titolare del trattamento
È assolutamente vietata qualsiasi manomissione agli apparati di telefonia mobile e alle sim di servizio.

2.4. INTERNET (dispositivi fissi e mobili, compresi cellulari di servizio, tablet,…)

L'utilizzo di internet è consentito esclusivamente per lo svolgimento delle proprie funzioni istituzionali.
La vasta gamma di attività istituzionali non permette la possibilità di definire un elenco di siti aziendali autorizzati, sono, comunque, utilizzati sistemi di filtraggio mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come palesemente estranei agli interessi ed alle attività istituzionali.
Il divieto di accesso ad un sito appartenente alle categorie inibite, viene visualizzato di norma e per certe categorie di siti, esplicitamente a video.
Il divieto riguarda, comunque, l'accesso a qualunque altro sito che, pur consentito dal sistema, non sia collegato o collegabile all'attività istituzionale dell'operatore.
Non è consentito lo scarico di software (vietato effettuare il "download" ed installare programmi dalla rete internet), file musicali o video da siti internet, se non espressamente autorizzato dal proprio titolare.
E' vietata ogni forma di registrazione a siti i cui contenuti non siano correlati all'attività lavorativa.
Non è permessa la partecipazione, per motivi non professionali, a forum, né l'utilizzo di chat line, di bacheche elettroniche nonché le registrazioni in guest book anche utilizzando pseudonimi (o nickname).
E' vietato utilizzare servizi di comunicazione e condivisione file (condivisione P2P "peer-to peer"), di file sharing, podcasting, streaming TV.
Non è consentito l'utilizzo delle risorse dei server aziendali per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa.
E' vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi direttamente autorizzati dal titolare del trattamento e funzionali alle attività istituzionali
E' vietato l'utilizzo di abbonamenti privati (connessioni analogiche e non) per effettuare la connessione a internet tranne in casi del tutto eccezionali e previa autorizzazione dal titolare del trattamento

2.5. RETE AZIENDALE

La rete informatica aziendale è protetta da un sistema di firewall perimetrale e da un sistema di antivirus centralizzato che aggiorna periodicamente le postazioni collegate alla rete.
E' comunque obbligo degli utenti mettere in essere tutte le procedure per garantirne il perfetto funzionamento e protezione della stessa.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi.
Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
Non è consentita la condivisione di archivi (data-base) se non espressamente autorizzata
Il titolare si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema informatico, ovvero acquisiti o installati in violazione della presente policy.
A tal fine si ricorda che vengono svolte attività di controllo. La rimozione è preceduta da una comunicazione all'utente interessato, fatta salva la possibilità di rimozione diretta in caso di immediato pericolo per la sicurezza del sistema informatico, dandone successivamente comunicazione all'utente interessato.
Nel caso il software antivirus segnali una anomalia, si dovranno sospendere le attività in corso ed informare tempestivamente il titolare che provvederà alle azioni del caso (es: informando l'amministratore di sistema)

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi; si elencano i più significativi:

- Clonare indirizzi macchina dei dispositivi autorizzati al collegamento alla rete Wi-Fi;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (User Id e Password) di accesso al sistema;
- violare la riservatezza di altri utenti;
- agire deliberatamente con attività che influenzano negativamente la regolare operatività della rete e ne riduca l'utilizzabilità e le prestazioni per altri utenti;
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (basi dati, software, ecc.);
- installare o diffondere su qualunque dispositivo e sulla rete, programmi destinati a danneggiare i sistemi o la rete (virus, spamming, worms, ecc.);
- cancellare, disinstallare, asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware;
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;

2.6. POSTA ELETTRONICA

La posta elettronica costituisce uno strumento di lavoro: le caselle e-mail sono utilizzate solo per i motivi attinenti alla propria attività lavorativa attraverso unicamente gli indirizzi forniti dal datore di lavoro o acquisiti presso clienti o utenti
Sono attivati indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse.
Al singolo utente può essere assegnato un indirizzo e-mail personale. La personalizzazione dell'indirizzo non comporta la sua "privatezza" in quanto trattasi di strumenti di esclusiva proprietà aziendale messi a disposizione del lavoratore al solo fine dello svolgimento delle proprie funzioni lavorative.
Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione del titolare.
E' obbligatorio controllare, anche tramite antivirus, gli allegati di posta elettronica prima del loro utilizzo.
Non eseguire download di files eseguibili o documenti da siti Web o Ftp non conosciuti, non aprire o cliccare su link presenti in mail di dubbia provenienza (che riferiscano di errori di sistema, premi in denaro, disattivazione di account,… ed ogni caso in cui siano richiesti i dati dell'utente) . Tale comportamento previene l'introduzione di virus o similari nel proprio PC e nella rete aziendale.
Non diffondere messaggi di posta elettronica di provenienza dubbia.
E' vietato partecipare a catene telematiche (cosiddette di "Sant'Antonio") Se si dovessero ricevere messaggi di tale natura, si deve darne comunicazione tempestiva. Non si devono in alcun caso attivare gli allegati di tali messaggi.
Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Gli utenti sono tenuti a svuotare periodicamente la casella di posta elettronica loro assegnata, onde evitare inutili occupazioni di spazio sul server gestore del sistema di posta.
Non è ammesso l'utilizzo di sistemi di webmail personali e private.
E' vietata la configurazione sul PC di account di posta elettronica che non facciano riferimento al dominio aziendale.
La diffusione massiva (spamming) di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, e solo su autorizzazione del titolare
Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, sarà opportuno valutare i destinatari che dovranno essere messi in copia (CC) o in copia nascosta (Ccn).
Per l'invio di messaggi e-mail a più destinatari, sfruttare la funzionalità destinatari in CCN, in modo che non possano essere individuati gli indirizzi e-mail personali degli altri destinatari attraverso la funzione di proprietà, salvo esplicita autorizzazione di questi ultimi.
Nei messaggi inviati tramite posta elettronica aziendale verrà accluso il testo "Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dalle disposizioni aziendali adottate in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate distruggerla e darne informazione all'indirizzo mittente".
E' obbligatorio l'utilizzo della posta elettronica ordinaria e certificata per fini istituzionali nel rispetto delle norme vigenti in materia.
E' obbligatorio utilizzare la posta elettronica, ove possibile, per le comunicazioni tra l'Azienda e i dipendenti nel rispetto delle norme vigenti in materia, in particolare, delle norme in materia di protezione dei dati personali.
Nei casi normativamente previsti deve essere utilizzata la posta elettronica certificata per le comunicazioni ai dipendenti se dotati di idonea casella di posta.
È obbligatorio procedere almeno ogni tre mesi provvedere alla pulizia degli archivi con cancellazione di file obsoleti, inutili, duplicati; si consiglia quotidianamente di provvedere nei termini descritti per il materiale che non sarà sicuramente più necessario
Ogni comunicazione dovrà essere caratterizzata dal rispetto dei soggetti coinvolti e di terzi.

Quanto sopra si applica anche alle comunicazioni sindacali, che dovranno avvenire tramite le mail attribuite alle sigle, evitando invece l'uso della mail personale istituzionale diretta del rappresentante.
Ciascun operatore può, utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e che contengano le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura organizzativa interessata.
L'invio di file contenenti dati personali, in particolare quelli sensibili, è ammessa se il documento risulta criptato o sottoposto a forma di securizzazione equivalente

2.7. SOLUZIONI PER GARANTIRE LA CONTINUITÀ LAVORATIVA (BUSINESS CONTINUITY)

Nel caso in cui un dipendente si assenti senza preavviso, un fiduciario, dallo stesso dipendente preventivamente nominato, potrà intervenire con il solo fine di garantire la continuità dell'attività lavorativa.

Ciascun incaricato dovrà pertanto provvedere a nominare il "Custode delle parole-chiave (password)" e preferibilmente anche di un suo sostituto in caso di assenza.

La funzione di "Custode delle parole-chiave (password)" prevede i seguenti compiti:

1) Ricevere da ciascun Incaricato utilizzatore di computer una busta, già chiusa e controfirmata, contenente una sola credenziale (coppia di parola-chiave o password e username o nomeutente o user-id). Se l'utente dispone di diverse credenziali, dovrà ricevere altrettante buste chiuse.
2) Ogni busta, naturalmente, dovrà riportare gli estremi identificativi dell'utente della credenziale e il riferimento alla funzione che la credenziale in essa contenuta svolge, ovvero il sistema di accesso alla quale essa fa riferimento, la data di consegna
3) La busta chiusa sarà controfirmata anche dal "Custode" e quindi custodita in luogo sicuro di cui il "Custode" sia l'unico detentore della chiave.
4) in caso di assenza prolungata dell'incaricato (o suo impedimento) che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il "Custode" aprirà la busta e ne consegnerà il contenuto al Titolare o all'Incaricato da loro delegato, facendosi rilasciare ricevuta. Avvertirà tempestivamente dell'intervento il detentore originario della parole-chiave, invitandolo anche a sostituirla immediatamente.
5) In caso di smarrimento della parola-chiave da parte del legittimo detentore della stessa, provvederà a restituirgli la sua busta e a ricevere subito dopo copia della nuova parola chiave in busta chiusa controfirmata.
6) verificare se l'incaricato ha provveduto alla modifica ed alla consegna della nuova busta. In caso di assegnazione di nuova parole-chiave dal tecnico informatico, verificare che l'Incaricato abbia immediatamente provveduto a inserirne una nuova.
7) Intervenire nel caso che riscontri anomalie o negligenze nella riservatezza della gestione chiavi da parte dei colleghi, richiamandoli cortesemente al corretto comportamento e invitandoli a sostituire immediatamente la parole-chiave che si fosse perduta minando, anche solo potenzialmente, i requisiti di sicurezza.

8) Segnalare al Titolare eventuali problematiche riferibili alla gestione delle parole-chiave.
9) Gestire gli eventuali codici di cifratura (se e quando utilizzati) in modo identico a quello descritto per le parole chiave, in modo da assicurarne la disponibilità come previsto nei casi 2) e 3).

Al "Custode" l'istituto, su richiesta, metterà a disposizione un cassetta chiudibile a chiave da conservare o in cassaforte o in armadio a chiusura sicura, o altra soluzione equivalente che garantisca un'adeguata condizione di sicurezza. Del contenitore esisteranno soltanto 2 chiavi, date rispettivamente al "Custode" e al suo sostituto.

2.8. PC PORTATILI E FISSI, TABLET ED ASSIMILABILI

Il posto di lavoro costituito da personal computer, notebook, tablet ed eventuali accessori sono messi a disposizione completi di quanto necessario per svolgere le proprie funzioni, pertanto, è vietato modificarne la configurazione.
L'utilizzo dei pc è consentito esclusivamente per lo svolgimento delle proprie funzioni istituzionali.
L'utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti (portatili) sia durante l'utilizzo sul luogo di lavoro (portatili e fissi).
Al PC portatile si applicano le stesse regole di utilizzo previste per i PC connessi alla rete aziendale, con particolare attenzione alla rimozione di eventuali file che non devono essere salvati o archiviati.
I PC portatili utilizzati all'esterno (convegni, corsi, eventi vari etc…), in caso di allontanamento devono essere custoditi in un luogo protetto.
Il PC non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
Nel caso di accesso a Internet tramite la rete aziendale:

- Utilizzare l'accesso in forma esclusivamente personale;
- Utilizzare la password in modo rigoroso;
- Disconnettersi dalla rete aziendale al termine della sessione lavoro.
- Collegarsi periodicamente alla rete interna per consentire l'aggiornamento dell'antivirus e dei software in genere

Non utilizzare abbonamenti internet privati per collegamenti alla rete.
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica.
Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
È imposto il divieto di installare sul proprio terminale software diverso da quello distribuito in azienda, senza espressa autorizzazione del titolare del trattamento.
È imposto il divieto di modificare le configurazioni impostate sul proprio pc.
È obbligatorio procedere almeno ogni tre mesi provvedere alla pulizia degli archivi con cancellazione di file obsoleti, inutili, duplicati.
I computer, inclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti;
il server dovrà essere costantemente collegato ad un gruppo di continuità che consente di escludere al perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica.

2.9. SUPPORTI MAGNETICI (HARD DISK ESTERNI-CHIAVETTE USB, FIRMA DIGITALE, CD..)

Ai supporti magnetici si applicano le stesse regole di utilizzo previste per gli strumenti elettronici per quanto applicabili.
Non è consentito l'utilizzo di supporti personali (non forniti dal Titolare)
L'utilizzo di supporti magnetici (cd, dvd, usb etc….) è consentito prestando la dovuta attenzione, custodendo con diligenza gli stessi e conservandoli nel rispetto delle misure di sicurezza in luogo sicuro ed accesso controllato.
Non lasciare cd, chiavette (e simili), cartelle o altri documenti a disposizione di estranei;
Riporre i supporti di archiviazione informatica in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
Ogni dispositivo magnetico di provenienza esterna alla azienda dovrà essere verificato mediante sistema antivirus prima del suo utilizzo e, nel caso venga rilevato un virus dovrà essere consegnato al Titolare e non utilizzato.
Tutti i supporti magnetici riutilizzabili contenenti dati personali, in particolare se sensibili e/o giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.
È vietato il riutilizzo (compresa la cessione/prestito,…) di una apparecchiatura senza prima averne eliminato i dati ivi contenuti (la sola cancellazione o formattazione non è sufficiente)
non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
È obbligatorio procedere almeno ogni tre mesi alla pulizia degli archivi con cancellazione di file obsoleti, inutili, duplicati.

2.10. TELEASSISTENZA

Relativamente all'attività di manutenzione remota su P.C. connessi alla rete aziendale il personale esterno autorizzato potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene previa autorizzazione (anche telefonica) da parte dell'utente interessato. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al P.C..
Viene fornita, su richiesta, una comunicazione informativa sullo strumento utilizzato, nonché le modalità del suo utilizzo per tutti gli utenti aziendali interessati.
Di tali connessioni sono conservati i log di accesso

2.11. MEMORIZZAZIONE FILE DI LOG DELLA NAVIGAZIONE INTERNET

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) che possono venire consultati in maniera aggregata ed anonima.

2.12. BRING YOUR OWN DEVICE (BYOD)

Chiamato anche bring your own technology (BYOT), bring your own phone (BYOP), e bring your own PC (BYOPC), in italiano: porta il tuo dispositivo, porta la tua tecnologia, porta il tuo telefono e porta il tuo pc - è un'espressione usata per riferirsi

alla possibilità di portare i propri dispositivi personali nel posto di lavoro, e usarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni.
Il BYOD consente la containerizzazione, vale a dire creare due ambienti diversi sullo stesso dispositivo, con dati aziendali e dati personali (chiamate, SMS, localizzazione GPS, ecc) rigorosamente separati, fin ad avere una Virtual Machine livello del sistema operativo controllata dall'IT aziendale, o nel firmware del processore (a livello hardware, al di sotto del sistema operativo), o ricorrere a soluzioni di hosted virtual desktop (HVD) o virtual mobile OS, con cui l'utente si collega alla Intranet aziendale ad applicazioni e dati che fisicamente risiedono su un server remoto.
Il termine è anche usato per descrivere le stesse pratiche applicati agli studenti che usano i loro dispositivi in ambito educativo.[1] È stato proposto di applicare il BYOD anche in Italia al mondo della scuola per ovviare alla scarsità di dotazione informatica e l'insufficienza dei fondi pubblici
Questa politica è intesa a proteggere la sicurezza e l'integrità dei dati e dell'infrastruttura tecnologica dell'azienda. Possono verificarsi eccezioni limitate alla politica a causa di variazioni di dispositivi e piattaforme.
I dipendenti e qualsiasi altro utente, devono accettare i termini e le condizioni stabiliti in questa politica per poter collegare i loro dispositivi alla rete aziendale.

Uso accettabile

La società definisce un uso aziendale accettabile come attività che sostengono direttamente o indirettamente la sua attività.
L'azienda definisce l'uso personale non accettabile nei tempi lavorativi (è quindi vietata ogni comunicazione personale, uso per ricreazione, come lo sono la lettura o il gioco).
Ai dipendenti è vietato accedere a determinati siti Web durante l'orario di lavoro / mentre sono connessi alla rete aziendale a discrezione dell'azienda. Tali siti Web includono, in maniera non esaustiva: siti pornografici, giochi on-line, negozi on line ad uso personale,…
Le funzioni di fotocamera e / o video dei dispositivi non sono disabilitate ma dovranno rispettare le indicazioni contenute nel presente documento
I dispositivi se connessi alla rete aziendale non possono essere utilizzati per:

- Conservare o trasmettere materiali illeciti
- Memorizzare o trasmettere informazioni riservate ad altro ente/soggetto
- Molestare gli altri
- Impegnarsi in attività commerciali esterne
- Eccetera.

Sono consentite le seguenti app: (includere un elenco dettagliato di app, quali meteo, app di produttività, Facebook, ecc., Che saranno consentite esclusivamente per uso didattico)
Non sono consentite app non scaricate tramite iTunes o Google Play, ecc.
I dipendenti possono utilizzare il proprio dispositivo mobile per accedere alle seguenti risorse di proprietà dell'azienda: e-mail, calendari, contatti, documenti, ecc.
L'azienda ha una politica di tolleranza zero per sms o e-mail durante la guida e solo le conversazioni a mani libere durante la guida, sono consentite.

Dispositivi e supporto

Sono consentiti smartphone compresi i telefoni iPhone, Android, Blackberry e Windows
Sono consentiti tablet inclusi iPad e Android.
I problemi di connettività sono supportati dall'IT; i dipendenti non dovrebbero contattare il produttore del dispositivo o il loro gestore per problemi relativi al sistema operativo o all'hardware quando utilizzato in modalità “lavoro”

I dispositivi devono essere presentati all'IT per la configurazione di app standard, come browser, software di produttività per ufficio e strumenti di sicurezza, prima che possano accedere alla rete.

Rimborso

La società non rimborserà il dipendente in nessuna misura, per quello che è stato il costo del dispositivo.
La società non rimborserà il dipendente per i seguenti addebiti: roaming, overage del piano, ecc.

Sicurezza

Per impedire l'accesso non autorizzato, i dispositivi devono essere protetti da password utilizzando le funzionalità del dispositivo e per accedere alla rete aziendale è necessaria una password complessa.
Il dispositivo deve bloccarsi con una password o un PIN se è inattivo per cinque minuti.
Dopo cinque tentativi di accesso falliti, il dispositivo si blocca e sarà necessario contattare l'IT per riottenere l'accesso.
Ai dispositivi Rooted (Android) o jailbroken (iOS) è severamente vietato l'accesso alla rete.
Ai dipendenti viene automaticamente impedito di scaricare, installare e utilizzare qualsiasi app che non compare nell'elenco delle app approvate della società.
Gli smartphone e i tablet che non sono nell'elenco dei dispositivi supportati dell'azienda non sono autorizzati a connettersi alla rete.
Gli smartphone e i tablet appartenenti a dipendenti che sono solo per uso personale non sono autorizzati a connettersi alla rete.
L'accesso dei dipendenti ai dati aziendali è limitato in base ai profili utente definiti dall'IT e applicati automaticamente.
Il dispositivo del dipendente può essere cancellato da remoto se

- il dispositivo viene perso,
- il dipendente interrompe il proprio impiego,
- l'IT rileva una violazione di dati o policy, un virus o una minaccia simile alla sicurezza dei dati aziendali e dell'infrastruttura tecnologica .

Rischi / Passività / Avvertenze

Mentre l'IT prenderà ogni precauzione per evitare la perdita dei dati personali del dipendente nel caso in cui debba cancellare un dispositivo da remoto, è responsabilità del dipendente prendere ulteriori precauzioni, come il backup di e-mail, contatti, ecc.
La società si riserva il diritto di disconnettere i dispositivi o disabilitare i servizi senza notifica.
I dispositivi smarriti o rubati devono essere segnalati alla azienda entro 24 ore.
I dipendenti sono poi responsabili di notificare al proprio gestore di telefonia mobile immediatamente dopo, la perdita di un dispositivo.
Si prevede che il dipendente utilizzi i propri dispositivi in modo etico in qualsiasi momento e aderisca alla politica di utilizzo accettabile della società come sopra indicato.
Il dipendente è personalmente responsabile di tutti i costi associati al proprio dispositivo.

Il dipendente si assume la piena responsabilità per i rischi inclusi, a titolo esemplificativo ma non esaustivo, la perdita parziale o totale dei dati aziendali e personali a causa di arresti anomali del sistema operativo, errori, virus, malware e / o altri errori hardware o software o programmazione errori che rendono il dispositivo inutilizzabile.
La società si riserva il diritto di intraprendere azioni disciplinari appropriate fino alla risoluzione del licenziamento per non conformità a questa politica.

2.13. POLICY BACKUP ATTIVO DEI DATI

Con cadenza settimanale è effettuato:

- il Backup incrementale automatizzato file di database con gestione set di backup, verificando l'aggiornamento del file replicato in cartella destinazione.
- Copia di archiviazione incrementale delocalizzata su server di backup con garanzia di sicurezza fisica e logica, con archiviazione delle ricevute di buon fine

Con cadenza mensile gli incaricati di primo livello eseguono:

- il test di ripristino delle copie di backup
- Verifica della disponibilità della copia delocalizzata

Tramite la seguente procedura:

a) porre il database in modalità off-line
b) eseguire una copia manuale del DB
c) eseguire il restore
d) verificare la funzionalità e l'aggiornamento del DB
e) ripristinare la copia manuale
f) riportare il DB on-line

Con cadenza semestrale gli incaricati di primo livello eseguono la sostituzione dei supporti rimovibili con un nuovo set di backup

La formazione è finalizzata a fornire le linee guida e la consapevolezza necessaria ad adottare il massimo grado di attenzione nell'esecuzione delle procedure stesse, oltre ad illustrare le tecniche che garantiscono il miglior livello di sicurezza.
La formazione viene somministrata dal Responsabile, e viene ripercorsa in ogni caso di nuovo Soggetto/i incaricato e/o d'innovazione tecnologica e procedurale.

2.14. MODALITÀ DI USO PERSONALE DI MEZZI INFORMATICI

Non sono previste modalità di uso personale di mezzi informatici dell'Azienda con pagamento o fatturazione a carico dell'interessato

2.15. POLICY SISTEMA DI VIDEOSORVEGLIANZA

Non sono presenti sistemi di videosorveglianza

2.16. CONTROLLI

Il titolare non effettua sistematicamente il controllo dei dipendenti (ad esempio non controlla la posta elettronica e la navigazione in internet dei dipendenti)
Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, il titolare si riserva di effettuare con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree, e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle finalità istituzionali);
- 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 all'osservanza delle regole può essere circoscritto agli operatori afferenti alla struttura organizzativa in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sul server aziendali attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa o a sue aree e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato);
- 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 all'osservanza delle regole può essere circoscritto agli operatori afferenti alla struttura organizzativa in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un'analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Il titolare si riserva la possibilità di un intervento di controllo diretto qualora si verifichino situazioni di particolare "pericolosità", in particolare nell'utilizzo di strumenti elettronici che minacciano la sicurezza del sistema informativo. Tale situazione di estremo danno giustifica la mancata possibilità di procedere ad un avviso come evidenziato nei precedenti punti, a favore della risoluzione immediata della minaccia.
Il Titolare, a cui afferisce l'utente che sia trovato in situazione di utilizzo indebito degli strumenti informatici, può chiedere una analisi del traffico di rete con rilevazione della tipologia di utilizzo, nonché una analisi dei dati memorizzati sul server, dandone informazione all'utente stesso.

2.17. FIRMA GRAFOMETRICA

Il titolare ha deciso di non inserire nel progetto di dematerializzazione e di semplificazione dei processi che sta perseguendo, anche la digitalizzazione di documenti istituzionali, che vengono quindi trasformati in documenti informatici che possono essere firmati con firma elettronica avanzata (FEA) in modalità grafometrica, con trattamento e conservazione dei dati biometrici.

3. POLICY USO STRUMENTI CARTACEI

Conservare sempre i dati del cui trattamento
si è incaricati in apposito armadio assegnato, dotato di serratura;
Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale (L'ubicazione di stampanti/fax e simili, non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale);
Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati (è vietata la riproduzione non autorizzata anche con cellulari e dispositivi simili);
Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati (tramite apposito distruggi documenti);
Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte (è quindi vietato il riuso di documenti contenenti dati personali);
Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;
Segnalare tempestivamente al collega interessato od al proprio superiore la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.
Si ricorda che la eliminazione di documenti contenenti dati personali deve avvenire tramite distruggitori di documenti
L'accesso agli archivi contenenti dati personali, è gestito da idonee procedure di sicurezza, che comprendono la possibile identificazione del soggetto che accede agli archivi, è quindi vietato l'accesso a chi non abbia esplicita autorizzazione
i documenti contenenti dati sensibili non devono essere lasciati incustoditi, quando sono affidati agli incaricati e si trovano all'esterno degli archivi protetti
durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta
La gestione del protocollo è eseguita mediante un apposito software e periodicamente (almeno mensilmente), l'incaricato di primo livello si preoccupa che i dati relativi ai protocolli vengano archiviati

4. POLICY GESTIONE CHIAVI (EDIFICIO, ARCHIVI, UFFICI,..)

L'accesso agli edifici, archivi, uffici,…, è gestito da idonee procedure di sicurezza, che comprendono la possibile identificazione del soggetto che accede: le chiavi sono affidate a personale autorizzato (o custode) che ne ha responsabilità di custodia ed è l'unico soggetto autorizzato a possederle

Pertanto l'Incaricato ad un trattamento dovrà rivolgersi di norma al "Custode" per ricevere la chiave necessaria ad accesso controllato.

Per le emergenze, si ricorda che copia delle chiavi saranno a disposizione anche del Titolare o di altri da lui delegati, però con le seguenti modalità che assicurino dell'uso esclusivamente per situazioni d'emergenza e della custodia con modalità di elevata sicurezza:

1) Una copia delle chiavi sarà collocata in apposito contenitore chiuso in custodia al Titolare oppure consegnate dal "Custode", al suo delegato, i quali avranno cura di conservarle in luogo sicuro e le utilizzeranno esclusivamente in caso di assenza del "Custode".
2) Il "Custode" terrà la chiave con sé o in luogo sicuro e la consegnerà temporaneamente solamente quando l'Istituto è aperto ed esclusivamente alle persone autorizzate secondo le indicazioni ricevute dal Titolare del trattamento
3) Dovrà altresì verificare che le chiavi siano a lui restituite dopo il tempo tecnico strettamente necessario all'accesso all'archivio.

5. POLICY GESTIONE ALLARMI

Contro i rischi d'intrusione i locali, sono dotati di impianto d'allarme, attivabile mediante digitazione d'un codice consegnato al personale dipendente.
È disposta l'attivazione dell'allarme al termine dell'orario di lavoro.
L'utilizzo dei sistemi di allarme antintrusione è gestito da idonee procedure di sicurezza, che comprendono la possibile identificazione del soggetto che ne fa uso; le chiavi ed i codici sono affidate a personale autorizzato che ne ha responsabilità di custodia ed è l'unico soggetto autorizzato a possederle

6. POLICY FOTO E VIDEO

È consentito effettuare fotografie e/o videoriprese che ritraggano l'alunno e/o i suoi familiari, CHE ABBIANO ESPLICITAMENTE AUTORIZZATO TALE TRATTAMENTO, durante lo svolgimento di attività didattiche afferenti ad attività istituzionali della scuola, inserite nel Piano dell'Offerta Formativa.

In ogni caso il trattamento avrà natura temporanea dal momento che le suddette immagini e/o video resteranno solo per il tempo necessario per la finalità cui sono destinati.
Nei video e nelle immagini di cui sopra i minori saranno ritratti solo nei momenti "positivi" legati alla vita della scuola.

I contesti autorizzati di pubblicazione e le motivazioni ritenute congrue per la pubblicazione delle foto o dei video sono dettagliate nella informativa privacy relativa alle foto e video

7. POLICY PERSONALE COLLABORATORE

Vedasi paragrafo "POLICY USO STRUMENTI CARTACEI"
Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:

- Registro personale dei docenti
- Registro di classe
- Certificati medici esibiti dagli alunni a giustificazione delle assenze
- Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti

Accertarsi che al termine delle lezioni tutti i computer dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi floppy disk, cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede e provvedendo temporaneamente alla loro custodia.
Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.

7.1. REGISTRO VISITATORI

È stato individuato il responsabile del registro dei visitatori, i suoi compiti sono quelli di controllare la corretta compilazione del registro e di provvedere alla eliminazione dei dati secondo le procedure stabilite (ogni 30 giorni tramite consegna del registro al titolare del trattamento che provvederà alla sua distruzione secondo le tempistiche indicate nel registro dei trattamenti)

8. POLICY PERSONALE DOCENTE

Vedasi paragrafo "POLICY USO STRUMENTI CARTACEI"

Custodire in apposito armadio dotato di serratura nella stanza individuata come sala professori dell'edificio i seguenti documenti:

- Registro personale
- Certificati medici esibiti dagli alunni a giustificazione delle assenze
- Qualunque altro documento contenente dati personali o sensibili degli alunni

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.

Tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax per il trattamento dei dati personali.

9. POLICY RESTORE E DISASTER RECOVERY

La previsione di Legge non solo richiede la puntuale esecuzione delle procedure di backup finalizzate alla conservazione dei dati, ma richiede anche la disponibilità degli stessi nel tempo e comunque per tutta la durata del servizio in erogazione. A tal riguardo è necessario poter dimostrare di aver agito e previsto, al meglio delle possibilità della struttura, le attività di ripristino della disponibilità del servizio a causa di evento distruttivo imprevedibile.
Tale procedura è definita di *Disaster Recovery* ed è in tal senso di tipica derivazione informatica peraltro prassi consolidata per i grandi data-center.

Considerata la gravità e l'eccezionalità degli eventi che possono generare l'adozione della procedura qui illustrata, si stabilisce di conferire incarico per l'esecuzione della procedura agli incaricati di primo livello, che , sentito il titolare, disporranno tempestivamente:

a) il blocco delle attività di trattamento
b) analisi dei danni subiti e relazione al Titolare
c) denuncia alle Autorità competenti ove previsto (vedasi "POLICY DATA BREACH") ed informativa agli interessati se il rischio per i diritti e le libertà risultano elevati
d) denuncia alla compagnie assicurative ove esista copertura
e) comunicazione ad Enti e/o Soggetti/Aziende coinvolti in ragione della proprietà immobiliare/mobiliare dei beni interessati dal disastro
f) Stima dei tempi di ripristino delle infrastrutture danneggiate
g) diffusione informativa sulla sospensione del servizio
h) Stima dei tempi di ripristino degli strumenti preposti al trattamento
i) Analizzare e predisporre se possibile, strumenti alternativi per il periodo di inattività forzosa
j) Comunicazione dei tempi di ripristino del servizio parziale o totale
k) Organizzare e supervisionare le procedure di acquisto e ripristino degli strumenti
l) Testare la compatibilità e l'affidabilità dei sistemi ripristinati
m) Convocare l'Incaricato della procedura di restore dei dati ed eseguire la stessa
n) Verificare la disponbilità di tutti i dati e dei corrispondenti servizi
o) Disporre il ripristino delle attività di trattamento
p) Comunicare il ripristino del servizio

Per situazioni di disastro che interessano le infrastrutture tecnologiche, si dispone di organizzare una configurazione minima di replica del sistema che prevede:

- Server delocalizzato con replica dell'active directory di dominio
- Client delocalizzato, configurato per l'accesso ai database e le utenze di base

Per le situazione di disastro che interessano i trattamenti non informatizzati, si dichiara la definitiva distruzione dei supporti in uso e si dispone l'utilizzo delle copie disponibili.

10. POLICY DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR.

Per **"Violazione di dati**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.
Nel caso in cui si verifichi uno degli eventi descritti nel presente capitolo o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare

immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al responsabile per la protezione dei dati personali (DPO).
Nel caso di un incidente informatico, dovrà essere compilata scheda su apposito registro. Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, ecc.).
In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- furto o smarrimento di laptop, smartphone, tablet aziendali contenenti Dati personali;
- furto o smarrimento di documenti cartacei contenenti Dati personali;
- furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- diffusione impropria di Dati personali, per mezzo di:
  - invio di e-mail contenente Dati personali al destinatario errato;
  - invio di e-mail con un file contenente Dati personali allegato erroneamente;
  - esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;

- richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

1. Rischio assente: la notifica al Garante non è obbligatoria.

2. Rischio presente: è necessaria la notifica al Garante.
3. Rischio elevato: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

1. coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
2. riguardare categorie particolari di dati personali;
3. comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
4. comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
5. impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).
6. il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
7. gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
8. sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
9. in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

NB: Se il data breach rientra in uno degli esempi di cui all'Annex B del documento 18/EN WP250rev.01, procedere secondo le indicazioni ivi riportate

11. POLICY TRASMISSIONE DATI

La trasmissione e/o divulgazione di dati deve avvenire con certezza di consegna al legittimo destinatario, è quindi buona prassi evitare di utilizzare strumenti che non garantiscono sufficiente grado di segretezza e certezza sulla precisa raggiungibilità.

Si segnalano come poco idonei al tal riguardo strumenti come:

- posta elettronica non certificata (tutta quella tradizionale)
- telefono (voce, sms, mms, ecc.)
- fax
- altri sistemi di trasmissione e messaggistica via web non certificati e criptati

Detti strumenti si possono utilizzare per sollecitare il contatto e/o mettere a conoscenza il legittimo destinatario delle disponibilità (in forma sicura) d'informazioni che lo riguardano.
Si consiglia di utilizzare quale strumenti sicuri:

- la trasmissione scritta in busta chiusa con consegna diretta all'interessato
- la comunicazione verbale in presenza del legittimo destinatario
- la diffusione via web in sessioni ad accesso riservato e criptato

In ogni caso è necessario verificare l'identità della persona tramite verifica della carta di identità o documento equivalente

12. POLICY SULL'ESERCIZIO DEI DIRITTI

Per favorire l'esercizio dei diritti dell'interessato in modo tempestivo e nell'ottica del maggior rispetto dei diritti soggettivi del medesimo, qualora l'interessato manifesti l'interesse all'esercizio dei propri diritti, è necessario adottare le seguenti linee guida:

- Gli interessati devono presentare le loro richieste al Titolare del trattamento;
- la richiesta deve essere presentata per iscritto, richiedendo l'apposito "modello esercizio diritti" prestampato messo a disposizione dal Titolare presso gli uffici di segreteria e su richiesta
- ogni incaricato deve agevolare la disponibilità di detto modello, a fronte di qualsiasi richiesta anche generica, che gli pervenga, anche verbale, a mezzo posta, per fax, per posta elettronica;
- la richiesta deve essere necessariamente accolta, senza che l'interessato debba presentare le proprie motivazioni;
- unico caso in cui è necessaria la motivazione riguarda l'opposizione per motivi legittimi;
- la richiesta può provenire anche da una persona fisica diversa dall'interessato o da un'associazione: in questo caso è necessario verificare la delega da parte dell'interessato;
- la risposta alle richieste avanzate deve giungere senza ritardo Entro un mese dalla richiesta formulata dall'interessato, provvedendo a fornire le informazioni relative alla azione intrapresa;
  NB: Soltanto in casi particolari, ad esempio quando le richieste siano molto numerose oppure le informazioni da fornire siano particolarmente complesse, il titolare potrà estendere questo termine ad un periodo massimo di due mesi, informando però, sempre entro un mese dalla sua richiesta, l'interessato della necessità di proroga e dei relativi motivi che l'hanno resa necessaria (per esempio, i tempi tecnici necessari al titolare per reperire le informazioni e per preparare la documentazione)
- si consiglia comunque di rispondere nel tempo più breve possibile dal deposito dell'istanza

- quando è richiesta la comunicazione in forma intellegibile dei dati personali dell'interessato si rileva che può essere effettuata con qualsiasi mezzo
- Le modalità di trasmissione delle informazioni (elettroniche, cartacee,…) devono essere concordate con l'interessato
- all'interessato vengono comunicate le sole informazioni di suo interesse (sono esclusi dati ulteriori, opinioni,…)

Il modello per l'esercizio dei diritti, deve essere messo a disposizione degli Interessati anche se non è obbligatoria la compilazione dello stesso, ma spiegando all'interessato che poter disporre di un formulario compilato, garantisce una migliore comprensione dell'espressione di volontà dell'Interessato e ne circoscrive l'ambito alle sole richieste indicate, fornendo la possibilità al titolare di rispondere in maniera quanto più precisa ed esaustiva possibile.

13. POLICY WISTEBLOWING

FONTE NORMATIVA E NATURA DELL'ISTITUTO

L'art. 1, comma 51, della legge 190/2012 (cd. legge anticorruzione) ha inserito un nuovo articolo, il 54 bis1, nell'ambito del d.lgs. 165/2001, rubricato "tutela del dipendente pubblico che segnala illeciti", in virtù del quale è stata introdotta nel nostro ordinamento una misura finalizzata a favorire l'emersione di fattispecie di illecito, nota nei paesi anglosassoni come whistleblowing. Con l'espressione whistleblower si fa riferimento al dipendente di un'amministrazione che segnala violazioni o irregolarità commesse ai danni dell'interesse pubblico agli organi legittimati ad intervenire. La segnalazione (cd. whistleblowing), in tale ottica, è un atto di manifestazione di senso civico, attraverso cui il whistleblower contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per l'amministrazione di appartenenza e, di riflesso, per l'interesse pubblico collettivo. Il whistleblowing è la procedura volta a incentivare le segnalazioni e a tutelare, proprio in ragione della sua funzione sociale, il whistleblower. Lo scopo principale del whistleblowing è quello di prevenire o risolvere un problema internamente e tempestivamente.

SCOPO E FINALITA' DELLA PROCEDURA

Scopo del presente documento è quello di rimuovere i fattori che possono ostacolare o disincentivare il ricorso all'istituto, quali i dubbi e le incertezze circa la procedura da seguire e i timori di ritorsioni o discriminazioni. In tale prospettiva, l'obiettivo perseguito dalla presente procedura è quello di fornire al whistleblower chiare indicazioni operative circa oggetto, contenuti, destinatari e modalità di trasmissione delle segnalazioni, nonché circa le forme di tutela che gli vengono offerte nel nostro ordinamento.

OGGETTO DELLA SEGNALAZIONE

Non esiste una lista tassativa di reati o irregolarità che possono costituire l'oggetto del whistleblowing. Vengono considerate rilevanti le segnalazioni che riguardano

comportamenti, rischi, reati o irregolarità, consumati o tentati, a danno dell'interesse pubblico. In particolare la segnalazione può riguardare azioni od omissioni, commesse o tentate:

- penalmente rilevanti;
- poste in essere in violazione dei Codici di comportamento o di altre disposizioni aziendali sanzionabili in via disciplinare;
- uscettibili di arrecare un pregiudizio patrimoniale all'amministrazione di appartenenza o ad altro ente pubblico;
- suscettibili di arrecare un pregiudizio all'immagine dell'azienda di appartenenza;
- suscettibili di arrecare un danno alla salute o sicurezza dei dipendenti, utenti e cittadini o di arrecare un danno all'ambiente;
- pregiudizio agli utenti o ai dipendenti o ad altri soggetti che svolgono la loro attività presso l'azienda.

Il whistleblowing non riguarda doglianze di carattere personale del segnalante o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro o rapporti col superiore gerarchico o colleghi, per le quali occorre fare riferimento alla disciplina e alle procedure di competenza del Servizio Personale e del Comitato Unico di Garanzia.

CONTENUTO DELLE SEGNALAZIONI

Il whistleblower deve fornire tutti gli elementi utili a consentire agli uffici competenti di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione. A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:

a) generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'azienda;
b) una chiara e completa descrizione dei fatti oggetto di segnalazione;
c) se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi;
d) se conosciute, le generalità o altri elementi (come la qualifica e il servizio in cui svolge l'attività) che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;
e) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
f) l'indicazione di eventuali documenti che possono confermare la fondatezza di tali fatti;
g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Le segnalazioni anonime, vale a dire prive di elementi che consentano di identificare il loro autore, anche se recapitate tramite le modalità previste dal presente documento, non verranno prese in considerazione nell'ambito delle procedure volte a tutelare il dipendente pubblico che segnala illeciti, ma verranno trattate alla stregua delle altre segnalazioni anonime e prese in considerazione per ulteriori verifiche solo se relative a fatti di particolare gravità e con un contenuto che risulti adeguatamente dettagliato e circostanziato. Resta fermo il requisito della veridicità dei fatti o situazioni segnalati, a tutela del denunciato.

MODALITA' E DESTINATARI DELLA SEGNALAZIONE

Per la segnalazione di condotte illecite (cosiddetto whistleblowing), ai sensi dell'art. 54 bis del d.lgs. n. 165/2001 così come modificato dalla legge n. 179/2017, è attiva una apposita sezione sul sito **dell'USR Lombardia.**

Il sistema è rivolto al whistleblower, ovvero il-la dipendente pubblico-a che intende segnalare illeciti di interesse generale e non di interesse individuale (vicende soggettive e personali di chi effettua la segnalazione), di cui sia venuto a conoscenza in ragione del rapporto di lavoro.

Link alla pagina esterna per la segnalazione delle condotte illecite: clicca qui

(http://usr.istruzione.lombardia.gov.it/amm-trasparente/whistleblower/)

Determinazione ANAC n. 6 del 28 aprile 2015

"Linee guida in materia di tutela del dipendente pubblico che segnala illeciti".

L'Azienda mette inoltre a disposizione dei propri dipendenti e dei propri collaboratori a qualsiasi titolo un apposito modello il cui utilizzo rende più agevole e rispondente ai requisiti della presente procedura. Il modello è reperibile sulla rete intranet nello spazio dedicato all'anticorruzione, sezione "Whistleblowing" ove sono altresì pubblicate le modalità di compilazione ed invio. La segnalazione può essere indirizzata:

a) al Responsabile per la prevenzione della corruzione,
b) al Responsabile dell'Ufficio per i procedimenti disciplinari istituito presso la Sede Legale;
c) al Responsabile della struttura di appartenenza.

La segnalazione presentata ad uno dei soggetti indicati alle lett. b) e c) o ricevuta da qualsiasi altro dipendente dell'Azienda deve essere tempestivamente inoltrata, a cura del ricevente e nel rispetto delle garanzie di riservatezza, al Responsabile per la prevenzione della corruzione al quale è affidata la sua protocollazione in via riservata e la tenuta del relativo registro. Qualora il whistleblower rivesta la qualifica di pubblico ufficiale, l'invio della segnalazione ai suddetti soggetti non lo esonera dall'obbligo di denunciare alla competente Autorità giudiziaria i fatti penalmente rilevanti e le ipotesi di danno erariale. La segnalazione può essere presentata con le seguenti modalità:

a) mediante invio, all'indirizzo di posta elettronica a tal fine appositamente attivato, whistleblowing@istitutopicopallino.it. In tal caso, l'identità del segnalante sarà conosciuta solo dal Responsabile della prevenzione della corruzione che ne garantirà la riservatezza, fatti salvi i casi in cui non è opponibile per legge;
b) a mezzo del servizio postale o tramite posta interna; in tal caso, per poter usufruire della garanzia della riservatezza, è necessario che la segnalazione

venga inserita in una busta chiusa che rechi all'esterno la dicitura "riservata/personale";

c) verbalmente, mediante dichiarazione rilasciata e riportata a verbale da uno dei soggetti legittimati alla loro ricezione;

ATTIVITA' DI VERIFICA DELLA FONDATEZZA DELLA SEGNALAZIONE

La gestione e la verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al Responsabile per la prevenzione della corruzione che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati. A tal fine, il Responsabile per la prevenzione della corruzione può avvalersi del supporto e della collaborazione delle competenti strutture aziendali e, all'occorrenza, di organi di controllo esterni all'azienda (tra cui Guardia di Finanza, Direzione Provinciale del Lavoro, Comando Vigili Urbani, Agenzia delle Entrate). Qualora, all'esito della verifica, la segnalazione risulti fondata, il Responsabile per la prevenzione della corruzione, in relazione alla natura della violazione, provvederà:

a) a presentare denuncia all'autorità giudiziaria competente;
b) a comunicare l'esito dell'accertamento al Responsabile della struttura di appartenenza dell'autore della violazione accertata, affinchè provveda all'adozione dei provvedimenti gestionali di competenza, incluso, sussistendone i presupposti, l'esercizio dell'azione disciplinare;
c) alla Direzione Aziendale e alle strutture competenti ad adottare gli eventuali ulteriori provvedimenti e/o azioni che nel caso concreto si rendano necessari a tutela dell'Azienda.

FORME DI TUTELA DEL WHISTLEBLOWER

A) Obblighi di riservatezza sull'identità del whistleblower e sottrazione al diritto di accesso della segnalazione Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non è opponibile per legge, (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo) l'identità del whisteblower viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata senza il suo espresso consenso e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazioni sono tenuti a tutelare la riservatezza di tale informazione. La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento. Per quanto concerne, in particolare, l'ambito del procedimento disciplinare, l'identità del segnalante può essere rivelata all'autorità disciplinare e all'incolpato solo nei casi in cui :
   - vi sia il consenso espresso del segnalante;
   - la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato, sempre che tale

circostanza venga da quest'ultimo dedotta e comprovata in sede di audizione o mediante la presentazione di memorie difensive.

La segnalazione del whistleblower è, inoltre, sottratta al diritto di accesso previsto dagli artt. 22 e seguenti della legge 241/1990 e ss.mm.ii.. Il documento non può, pertanto, essere oggetto di visione né di estrazione di copia da parte di richiedenti, ricadendo nell'ambito delle ipotesi di esclusione di cui all'art. 24, comma 1, lett. a), della l. n. 241/90 s.m.i..

B) Divieto di discriminazione nei confronti del whistleblower Nei confronti del dipendente che effettua una segnalazione ai sensi della presente procedura non è consentita, né tollerata alcuna forma di ritorsione o misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. Per misure discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili. La tutela è circoscritta alle ipotesi in cui segnalante e denunciato siano entrambi dipendenti. Il dipendente che ritiene di aver subito una discriminazione per il fatto di aver effettuato una segnalazione di illecito deve dare notizia circostanziata dell'avvenuta discriminazione
   - al Responsabile della prevenzione della corruzione che, valutata la sussistenza degli elementi, segnala l'ipotesi di discriminazione: al Responsabile della struttura di appartenenza del dipendente autore della presunta discriminazione. Il Responsabile della struttura valuta tempestivamente l'opportunità/necessità di adottare atti o provvedimenti per ripristinare la situazione e/o per rimediare agli effetti negativi della discriminazione in via amministrativa e la sussistenza degli estremi per avviare il procedimento disciplinare nei confronti del dipendente autore della discriminazione;
   - all'Ufficio che per i procedimenti di propria competenza, valuta la sussistenza degli estremi per avviare il procedimento disciplinare nei confronti del dipendente che ha operato la discriminazione;
   - al Servizio Legale dell'Azienda, che valuta la sussistenza degli estremi per esercitare in giudizio l'azione di risarcimento per lesione dell'immagine della Azienda;
   - all'Ispettorato della funzione pubblica. Resta ferma la facoltà del dipendente di rivolgersi direttamente al Comitato Unico di Garanzia che provvederà a darne tempestiva comunicazione al Responsabile per la prevenzione della corruzione.

RESPONSABILITA' DEL WHISTLEBLOWER

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare del whistleblower nell'ipotesi di segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 del codice civile. Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente policy, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di

utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

14. DISPOSIZIONI FINALI

Per quanto non espressamente previsto nella presente policy sarà fatto riferimento alla normativa vigente in materia. La presente policy sarà diffusa quanto più possibile, dandone contestuale informazione a tutti gli utenti. E' fatto obbligo di adeguare i propri comportamenti alle disposizioni previste nella presente policy ed a chiunque competa di osservarla

14.1. PROVVEDIMENTI DISCIPLINARI

Qualora, ad esito di controllo o nell'effettuazione di attività di manutenzione, nel rispetto delle procedure di cui al presente documento, si rilevino delle anomalie, che possano essere configurate quali attività non conformi, si valuterà l possibilità di procedere ad azione disciplinare

Il titolare, procederà a tutti i successivi adempimenti nel rispetto delle disposizioni normative, contrattuali e regolamentari vigenti in materia.

L'Azienda procederà altresì a segnalare, eventualmente, l'evento alle Autorità competenti, anche al fine di una potenziale valutazione del danno erariale.

Qualora la tipologia, la quantità o la modalità di anomalie riscontrate, siano tali da essere rilevanti ai fini del codice penale, provvederà obbligatoriamente ad effettuare specifica denuncia all'Autorità Giudiziaria.