Regolamento d'Istituto per l'utilizzo dei dati personali e degli strumenti di trattamento

rev 1912

Modello R2.1 Allegato alle autorizzazioni ai trattamenti

REGOLE GENERALI

Gli Incaricati devono attenersi rigorosamente a tutte le regole dettate dalla normativa di riferimento (ad oggi D.Lgs.196/2003 o Codice, Regolamento UE 2016/679 o GDPR, provvedimenti del Garante, codice AgID) e in particolare ai seguenti punti fondamentali:

L'obbligo di mantenere il dovuto **riserbo 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 (art.326 del codice penale e art. 28 della legge 241/90).

Ai sensi dell'art. 29 del GDPR e dell'articolo 2-quaterdieces del Codice gli Incaricati del trattamento devono operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) e devono elaborare i dati personali ai quali hanno accesso **attenendosi alle istruzioni impartite**.

Finalità del trattamento: il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali, per finalità e con modalità previste da leggi o regolamenti.

Modalità di trattamento dei dati sensibili/giudiziari: Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, i documenti (anche tuttora in lavorazione e non definitivi) ed i supporti recanti dati sensibili o giudiziari devono essere conservati in elementi di arredo o ambienti muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato. In caso di trattamento elettronico, tali documenti devono essere inviati per la conservazione sui sistemi in dotazione all'Istituto (server, aree di condivisione) e cancellati dai dispositivi eventualmente utilizzati per la redazione o la visualizzazione.

Trattamenti di dati inerenti la salute: i supporti ed i documenti recanti dati relativi alla salute, dati genetici o biometrici e dati relativi alle abitudini sessuali devono essere conservati separatamente dai dati comuni, preferibilmente in contenitori muniti di serratura o, in caso di trattamento elettronico, in cartelle ad accesso limitato.

Norme generali di comportamento

- assicurarsi che quando parla con altri, personalmente o per telefono, relativamente a dati o situazioni tramite le quali sia identificabile un soggetto tutelato non siano presenti nell'ambiente terzi che non siano a loro volta incaricati del trattamento;

- i documenti vanno utilizzati prevalentemente negli ambienti deputati alle elaborazioni. Quando si renda necessario l'utilizzo in altri ambienti non lasciare i documenti incustoditi e, al termine, riportarli nel luogo dove devono essere conservati;
- nei luoghi di trattamento ai quali possono accedere anche soggetti non incaricati non lasciare i documenti accessibili in caso di assenza ma riporli nei dispositivi deputati (armadi, cassetti, classificatori). Ove sia prevista la chiusura con chiave dei dispositivi di conservazione fare in modo che venga utilizzata e che venga poi riposta nei modi che il Dirigente indicherà;
- nei luoghi di trattamento non accessibili al pubblico non assentarsi senza avere chiuso i locali. Nel caso si fosse impossibilitati a chiudere, assicurarsi che i documenti siano stati riposti;
- in caso il trattamento preveda lo spostamento dei documenti ad altra sede, fare in modo che il trasporto avvenga in regime di sicurezza: non lasciare i documenti incustoditi (in macchina, sui mezzi pubblici), non lasciare i documenti visibili da altri, non affidare a terzi, se non autorizzati, il trasporto;
- in caso di richiesta verbale, telefonica o scritta di dati riferibili ad un interessato assicurarsi che il richiedente sia autorizzato, ovvero che sussista un obbligo di legge, che esista un contratto con l'interessato che preveda la comunicazione a quel soggetto, che l'interessato abbia già espresso il suo consenso.
- se la comunicazione descritta al punto precedente non fosse consentita valutare con il Dirigente se sia il caso di richiedere un apposito consenso all'interessato. In tal caso raccogliere il consenso in forma scritta e conservarlo unitamente alla pratica;
- i documenti, o copie di essi, che non vengono più utilizzati devono essere distrutti ovvero resi illeggibili prima del loro cestinamento.

Diritti degli incaricati nell'utilizzo della posta elettronica e della navigazione web

Premessa

Il presente allegato recepisce le indicazioni e le raccomandazioni fornite dal Garante per la protezione dei dati personali in occasione della pubblicazione del Provvedimento del 1 marzo 2007 (registro delle deliberazioni n. 13 del 1 marzo 2007, pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007) in merito alla regolamentazione dell'uso della posta elettronica ed internet sul luogo di lavoro al fine di individuare un punto di equilibrio tra i diritti del datore di lavoro e quelli del lavoratore e di definire le regole comportamentali per un utilizzo lecito e corretto della Posta elettronica.

Il provvedimento Generale del Garante per la privacy marzo 2007

Il Provvedimento, il cui testo integrale è a disposizione sul sito web dell'Istituto, ribadisce due concetti fondamentali apparentemente in contrasto fra di loro:

a) il diritto del lavoratore a che sia rispettata la propria dignità e la propria riservatezza
b) il dovere del datore di lavoro di adottare idonee misure di sicurezza al fine di ridurre al minimo i rischi di perdita dei dati contenuti sul sistema informatico, di accesso non autorizzato agli strumenti informatici, di trattamenti non conformi o potenzialmente pericolosi sia per il sistema informatico che per l'integrità dei dati in esso contenuti.

Al fine di poter assolvere il proprio dovere di vigilanza sull'integrità del sistema informatico e del patrimonio informativo in generale il datore di lavoro non può, soprattutto in fase di

monitoraggio delle attività, ricavare informazioni relative al dipendente o collaboratore e a operazioni da lui effettuate, senza una serie di prerequisiti indispensabili.

Istruzioni

È senz'altro compito del datore di lavoro definire:

a) modalità di utilizzo delle risorse informatiche;
b) limiti all'utilizzo delle risorse informatiche;
c) margini discrezionali per consentire o negare l'utilizzo degli strumenti per finalità non direttamente collegate alle mansioni affidate al dipendente o collaboratore.

L'insieme delle misure di sicurezza e delle pratiche operative adottate deve essere portato a conoscenza del dipendente o collaboratore; questi è tenuto ad applicare quanto stabilito dal datore di lavoro collaborando per quello che per il suo ruolo è stato previsto.

Limitazioni

Quando il solo impartire istruzioni operative non si rivelasse sufficiente a limitare un uso non corretto degli strumenti elettronici il datore di lavoro può adottare quegli accorgimenti tecnici che limitino la discrezionalità del dipendente o collaboratore impedendo alcune operazioni o consentendone un numero limitato. Questa soluzione è caldeggiata dal garante stesso con la motivazione che vengono in questo modo limitate le occasioni nelle quali si concretizzi la necessità di effettuare controlli e monitoraggi sulle attività di un operatore.

Controlli

Adottando misure di sicurezza e procedure operative efficaci, inserendo nel sistema informatico strumenti che governino i margini di operatività degli operatori, si riducono al minimo le necessità di analizzare nel dettaglio le attività degli operatori. Tuttavia questa necessità può sussistere.
I controlli, per essere validi, devono rispettare il criterio di gradualità e di pertinenza o non eccedenza. Il garante non ammette controlli "a tappeto", cioè prolungati, indiscriminati e costanti.
La possibilità di accedere alla posta elettronica contenuta nelle caselle in dotazione al dipendente o collaboratore, o alla cronologia di navigazione web effettuata, deve essere definita in relazione alle possibilità operative concesse all'operatore stesso. La possibilità, o meno, di utilizzare la posta o la navigazione web per attività personali deve essere definita e portata a conoscenza del dipendente o collaboratore.

Nei prossimi paragrafi vengono quindi portate a conoscenza degli operatori le modalità di utilizzo della navigazione Internet, dell'utilizzo della posta elettronica e delle possibilità di accesso e di controllo da parte delle funzioni aziendali preposte.

Regolamento per l'utilizzo della posta elettronica

Ambito di applicazione

La presente procedura si applica nell'ambito dell'utilizzo della Posta elettronica per lo svolgimento delle proprie mansioni lavorative.

L'accettazione e la stretta osservanza del presente Regolamento è condizione essenziale per ottenere l'attribuzione in uso di una casella e-mail sui seguenti domini:

@istitutomantegna.it

Responsabilità

L'utilizzo della posta elettronica è fornito al personale a beneficio dell'intera organizzazione, del personale, degli utenti, dei fornitori e di tutti i soggetti con cui l'Istituto intrattiene rapporti di comunicazione.

Tale possibilità, infatti, consente di comunicare velocemente incrementando così la propria produttività.

Il personale ha la responsabilità di salvaguardare e migliorare l'immagine pubblica dell'organizzazione e di utilizzare la posta elettronica per finalità legittime ed etiche, in stretta connessione allo svolgimento delle proprie mansioni.

Tutti gli utenti del servizio di Posta elettronica (Responsabili, Incaricati o Utenti di rete) sono responsabili dell'applicazione rigorosa del presente Regolamento. L'amministratore di sistema ha l'obbligo di vigilare, nel rispetto dell'articolo 4 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), sulla corretta applicazione della presente procedura da parte di tutto il personale dell'organizzazione, evidenziando le eventuali criticità rispetto a quanto disposto e proponendo al Titolare le soluzioni ritenute più idonee data la struttura dell'organizzazione.

Modalità operative

In primo luogo si premette che tutte le informazioni archiviate negli elaboratori (inclusi documenti, altri file, messaggi di posta elettronica e le registrazioni dei messaggi di posta vocale) sono di proprietà dell'Istituto.

Ciò vale anche per la posta elettronica di tutti gli account dei domini sopra elencati (sia nominativi, es. nome.cognome@istituto....., che di funzione, es. segreteria@istituto.....)

Gli Utenti dei servizi di posta elettronica devono essere consapevoli che tutte le comunicazioni inviate o ricevute mediante i sistemi di posta elettronica per finalità di lavoro devono quindi essere considerate informazioni di carattere non riservato nei confronti dell'Istituto.

Ogni ulteriore informazione, materiale, comunicazione creata, spedita o recuperata attraverso la rete Internet per finalità estranee a quelle di lavoro è da ritenersi abusiva, in quanto eccedente e non pertinente alle finalità del trattamento affidate agli Incaricati.

L'attribuzione ad un utente di uno o più indirizzi di posta, personale (qualsiasi combinazione di nome e cognome) o identificativo della funzione e del ruolo all'interno dell'organizzazione è autorizzata per un uso esclusivamente professionale.
L'organizzazione, nel caso di cessazione del rapporto di lavoro o di assenze prolungate (ad esempio, per malattia o maternità) del lavoratore, si riserva il diritto di trattenere copia dei messaggi

e di potervi accedere, per garanzie di continuità dei rapporti con i terzi, ovvero di accertamento preventivo o difensivo di fatti illeciti.
Le modalità di gestione dei messaggi che verranno indirizzati alla casella di posta nominale di un utente che abbia cessato il rapporto di collaborazione o che rimanga assente per un tempo prolungato verrà concordata fra il dipendente o collaboratore stesso, il suo responsabile di funzione e l'amministratore di sistema. I termini dell'accordo saranno accettati e sottoscritti dal dipendente o collaboratore e applicati dall'amministratore di sistema.

L'utilizzo della casella di posta è vincolato alla immissione delle credenziali di autenticazione fornite. Tali credenziali possono essere preimpostate nell'applicativo fornito sul PC in dotazione o nel dispositivo portatile autorizzato.

L'eventuale utilizzo di procedure webmail autorizzate da Personal Computer al di fuori della struttura (internet point, casa) dovrà rispettare le regole fornite ai punti seguenti per tali modalità di utilizzo.

Gli Utenti dei servizi di posta elettronica devono utilizzare i sistemi a disposizione esclusivamente per ragioni professionali.
È consentito un limitato uso personale della posta elettronica purché non in contrasto con le disposizioni del presente regolamento e con lo svolgimento delle mansioni assegnate. Il dipendente o collaboratore, ricevendo il regolamento, viene portato a conoscenza che gli amministratori di sistema hanno accesso, nei limiti e per le finalità in esso dichiarate, agli archivi di posta.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi a disposizione per creare o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, insulti, epiteti ovvero qualsiasi altro contenuto o testo che possa essere considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi a disposizione per sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività aziendale.

Gli Utenti dei servizi di posta elettronica non devono tentare di rappresentare la posizione dell'organizzazione, mediante l'uso di sistemi di posta elettronica, su qualsiasi questione di carattere pubblico attraverso forum di discussione, salvo per l'esecuzione di attività di natura professionale, e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'organizzazione.

Gli Utenti dei servizi di posta elettronica devono vigilare al fine di evitare la rivelazione attraverso e-mail, news-group o forum pubblici di informazioni confidenziali.

Gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi a disposizione per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'organizzazione.

Gli Utenti dei servizi di posta elettronica sono responsabili in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio da essi pubblicati o trasmessi attraverso i sistemi di posta elettronica per finalità non strettamente correlate alla mansione assegnata.

In ogni caso gli Utenti dei servizi di posta elettronica non possono utilizzare i sistemi a disposizione per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie, o altro materiale appartenente ad altre organizzazioni, salvo per l'esecuzione di attività di natura professionale.

La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari dell'organizzazione ovvero ad azioni legali dei legittimi titolari del diritto d'autore nei confronti di chi si è reso responsabile di tali atti.

Gli Utenti dei servizi di posta elettronica, in considerazione degli obblighi e dei doveri precedentemente descritti, **possono accedere**, nei limiti e secondo le modalità descritte nel successivo "Regolamento per l'utilizzo di Internet", **alla propria casella di posta elettronica personale mediante l'utilizzo di procedure di webmail** per l'invio e il ricevimento di messaggi di posta elettronica di natura strettamente personale, **senza memorizzare il proprio account o le proprie credenziali.**

È vietato, salvo autorizzazione del Responsabile dei trattamenti su richiesta motivata da parte dell'utente o del responsabile di funzione approvata dall'amministratore di sistema della struttura di riferimento, l'utilizzo di applicativi per la gestione della posta elettronica diversi da quello adottato dall'Istituto.

In caso di assenza preventivata (ad es., per ferie o attività di lavoro fuori sede) gli Utenti dei servizi di posta elettronica dovranno impostare il proprio programma in modo che possa inviare automaticamente messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. Le modalità di impostazione del sistema di posta elettronica secondo quanto descritto sono richiedibili all'amministratore di sistema. Altre modalità di gestione dei messaggi in caso di assenza (inoltro ad altro indirizzo, nomina di un fiduciario che possa accedere alla casella di posta o ricevere in copia i messaggi) dovranno essere concordate con l'amministratore di sistema della struttura di riferimento.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il Titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre, lecitamente, mediante l'azione degli Amministratori di Sistema, l'attivazione di un analogo accorgimento, avvertendo gli interessati.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'utente potrà delegare, anche preventivamente, un collega (cosiddetto "fiduciario") a verificare il contenuto di messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il Fiduciario o il Titolare provvederanno a verbalizzare tale attività e ad informare il lavoratore interessato alla prima occasione utile.

Infine, i messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.
L'Istituto precisa, in accordo con i propri operatori, che le caselle di posta elettronica utilizzate, sia generiche (es. info, amministrazione) che nominali (nome.cognome, n.cognome) non devono essere utilizzate per messaggi di natura personale o riservata in quanto i messaggi ricevuti o inviati possono essere analizzati dalle funzioni aziendali a ciò preposte per ragioni di sicurezza. In caso di assenza prolungata di un operatore i messaggi a lui indirizzati vengono letti da altre funzioni

aziendali. In caso sia necessario attivare canali di comunicazione riservati si prega di contattare direttamente l'operatore interessato.

Il testo è richiedibile al Titolare.

Gli Utenti dei servizi di posta elettronica che abbiano notizia di una qualsiasi violazione della presente procedura sono tenuti a darne comunicazione al proprio Titolare. Gli Utenti dei servizi di posta elettronica che contravvengano alla presente procedura ovvero utilizzano l'utenza di posta elettronica aziendale per scopi impropri sono soggetti a sanzioni secondo quanto previsto dal contratto di lavoro di riferimento e/o da quanto previsto dalle vigenti normative e/o da regolamenti interni.

Regolamento per l'utilizzo della rete internet

Obiettivo

Il presente Regolamento si pone l'obiettivo di fornire le regole comportamentali per un utilizzo lecito e corretto della rete Internet.

Ambito di applicazione

Il presente Regolamento si applica nell'ambito dell'utilizzo della rete Internet sia per lo svolgimento delle proprie mansioni lavorative sia per il limitato e consentito uso personale di tale strumento di lavoro.

L'accettazione e la stretta osservanza del presente Regolamento è condizione essenziale per ottenere l'attribuzione in uso del servizio di accesso a Internet mediante IP pubblici attribuiti alla responsabilità dell'ente.

Responsabilità

L'accesso alla rete Internet è stato fornito al personale dell'organizzazione a beneficio dell'intera organizzazione. Tale possibilità consente al personale di usufruire di risorse informative sparse in tutto il mondo e di incrementare così la propria produttività.

Il personale ha la responsabilità di salvaguardare e migliorare l'immagine pubblica dell'organizzazione, e di utilizzare la rete Internet per finalità legittime, etiche e strettamente necessarie allo svolgimento delle mansioni lavorative. Al fine di assicurare che tutti i responsabili, dipendenti/utenti di rete siano utenti responsabili della rete Internet, utenti produttivi e attenti alla salvaguardia dell'immagine pubblica dell'organizzazione, è stata predisposto il presente Regolamento relativo all'utilizzo della rete Internet e/o degli accessi alla stessa attraverso la rete durante l'orario di lavoro. Pertanto, tutti gli utenti (Responsabili, Incaricati o Utenti di rete) sono responsabili dell'applicazione rigorosa del presente Regolamento.

Gli amministratori di sistema della struttura di riferimento hanno l'obbligo di vigilare, nel rispetto dell'articolo 4 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), sul rispetto della presente procedura da parte di tutto il personale dell'organizzazione.

Modalità operative

Gli utenti abilitati all'utilizzo della rete che hanno accesso alla rete Internet devono utilizzare questo strumento esclusivamente per ragioni professionali.

E' consentito l'uso a fini personali esclusivamente per l'accesso alla propria casella privata di posta tramite il web (cosiddette webmail), con periodicità tale da non inficiare l'attività lavorativa.

Le prescrizioni – riportare in questo Regolamento – sui contenuti ed i materiali veicolati tramite rete Internet devono essere rispettate anche con riferimento alla web mail privata, poiché vengono utilizzate risorse dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete possono utilizzare le normali risorse web e ftp della rete Internet esclusivamente per condurre affari aziendali ufficiali, ottenere pareri tecnici o analitici, per accedere ad informazioni relative alle attività dell'organizzazione o comunque correlate agli affari condotti dall'organizzazione. Non è consentito l'utilizzo di piattaforme di scambio peer to peer o di download continuativi, salvo esplicita autorizzazione del responsabile di funzione per comprovata necessità di servizio. In questo caso la procedura verrà impostata dall'Amministratore di Sistema.

Gli utenti abilitati all'utilizzo della rete non devono tentare di rappresentare la posizione dell'organizzazione su qualsiasi questione di carattere pubblico attraverso forum di discussione, salvo per l'esecuzione di attività di natura professionale e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete devono vigilare al fine di evitare la rivelazione di informazioni confidenziali attraverso e-mail, news-group o forum pubblici.

Gli utenti abilitati all'utilizzo della rete, al fine di evitare la propagazione di virus per elaboratori attraverso i sistemi aziendali, non possono effettuare il download di alcun software dalla rete Internet senza specifica autorizzazione da parte dell'Amministratore di Sistema. Dove sia tecnicamente possibile e non in conflitto con il normale utilizzo della risorsa informatica in dotazione questa funzione verrà disattivata dall'Amministratore di Sistema. Tutti i download di software dovranno essere approvati e materialmente compiuti dagli Amministratori di Sistema che provvederanno poi alla distribuzione e all'installazione, se prevista.

Gli utenti abilitati all'utilizzo della rete possono accedere alla rete Internet mediante la rete dell'Istituto durante l'orario di lavoro esclusivamente per attività nell'interesse dell'organizzazione e, sporadicamente, ad uso personale con i limiti riportati nella presente procedura.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete sono responsabili in via esclusiva del contenuto di messaggi, file di testo, immagini, file audio da essi pubblicati o trasmessi attraverso la rete Internet per finalità non strettamente correlate alla mansione assegnata.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare Internet per immettere in Rete (upload) ovvero ricevere (download) materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie o altro materiale appartenente ad organizzazioni diverse dall'organizzazione, salvo per l'esecuzione di attività legittime di natura professionale. La mancata osservanza del diritto d'autore, ovvero di accordi di licenza, può condurre ad azioni disciplinari dell'organizzazione o ad azioni legali dei legittimi titolari del diritto d'autore.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per creare o trasmettere materiale con contenuti sessuali espliciti, denigratori, diffamatori, osceni od offensivi, quali, a titolo esemplificativo, denigrazioni, epiteti ovvero qualsiasi altro contenuto o testo che possa essere considerato una molestia ovvero una discriminazione fondata sull'origine razziale, il

colore della pelle, la nazionalità, il sesso, preferenze sessuali, età, infermità fisiche o psichiche, stato di salute, stato civile rispetto al matrimonio, convinzioni politiche o religiose.

Gli utenti abilitati all'utilizzo della rete non possono utilizzare la rete Internet per sollecitare o fare proseliti per finalità commerciali, a beneficio di organizzazioni esterne, per catene di lettere, ovvero per altre finalità estranee all'attività dell'organizzazione.

Gli utenti abilitati all'utilizzo della rete devono essere consapevoli che tutte le comunicazioni create, spedite o recuperate dalla rete Internet per finalità di lavoro sono di proprietà dell'organizzazione e devono essere considerate informazioni di carattere pubblico.

Si ricorda che ogni informazione, materiale, comunicazione creata, spedita o recuperata attraverso la rete Internet per finalità estranee a quelle di lavoro è da ritenersi abusiva in quanto eccedente e non pertinente alle finalità del trattamento affidate agli Incaricati.

Attraverso la rete Internet è possibile accedere a siti che richiedono il versamento di quote di sottoscrizione o di utilizzo al fine di accedere alle informazioni disponibili sul sito. Gli Incaricati e gli Utenti di rete devono inoltrare al proprio Responsabile le richieste per l'approvazione di tali versamenti.

Gli utenti abilitati all'utilizzo della rete che abbiano notizia di una qualsiasi violazione della presente procedura è tenuto a darne comunicazione all'Amministratore di Sistema competente o al responsabile dei trattamenti.

Gli utenti abilitati all'utilizzo della rete che contravvengano alla presente procedura ovvero utilizzano l'accesso alla rete Internet per scopi impropri sono soggetti a sanzioni secondo quanto previsto dal contratto di lavoro di riferimento e/o da quanto previsto dalle vigenti normative e/o da regolamenti interni.

Gli amministratori di sistema della struttura di riferimento hanno l'obbligo di vigilare, nel rispetto dell'articolo 4 della L. 20 maggio 1970, n. 300 (Statuto dei lavoratori), sul rispetto della presente procedura da parte di tutto il personale dell'organizzazione.

R2.2 Allegato alle autorizzazioni ai trattamenti

Misure di sicurezza organizzative e tecniche

Chiunque operi sotto l'autorità del Titolare deve applicare, nel trattamento di dati personali, le misure di sicurezza, anche comportamentali, adottate e portate a conoscenza degli incaricati con le modalità che di volta in volta il Titolare stabilisce.

La normativa di riferimento è composta da D.Lgs.196/2003 o Codice, Regolamento UE 2016/679 o GDPR, provvedimenti del Garante, codice AgID.

Nel definire le misure di sicurezza e le regole per applicarle, sono state tenute in considerazione anche le "migliori pratiche" in tema di sicurezza informatica, relativamente alla tipologia di dispositivi utilizzati nel nostro Istituto. Il quadro di riferimento, sia legislativo che tecnico, è in continua evoluzione, quindi il presente regolamento verrà costantemente aggiornato e condiviso con tutti gli incaricati.

Utilizzo di documenti

Particolare attenzione deve essere riposta nell'utilizzo di documenti, in formato elettronico o cartaceo, che contengano dati o informazioni riconducibili ad uno o più interessati.

Non è consentito l'utilizzo di tali documenti fuori dal luogo di lavoro. Non sono ammesse copie, con qualsiasi modalità, anche parziali, che mantengano la possibilità di identificare gli interessati.

I documenti cartacei e le stampe di documenti elettronici, utilizzati all'interno del luogo di lavoro, devono essere riposti, riconsegnati agli incaricati addetti alla conservazione o distrutti, se non più necessari.

I documenti prodotti in formato cartaceo e non più utilizzabili, possono essere smaltiti negli appositi contenitori solo dopo essere stati resi illeggibili mediante il passaggio nei dispositivi trita carta, se in dotazione, o con altre modalità parimenti efficaci.

L'utilizzo di memorie di massa (flash drive, dischi USB) eventualmente in dotazione all'Istituto, utilizzate al fine di conservare temporaneamente documenti, dati o informazioni, deve prevedere l'applicazione di un sistema di crittografazione, impostato dall'amministratore di sistema o da un ruolo interno a cui venga affidato questo compito, che ne renda impossibile l'utilizzo su dispositivi non autorizzati o in mancanza di inserimento di una credenziale di de-crittografazione.

Accesso ai locali di trattamento o a dispositivi di conservazione

L'accesso ai locali di trattamento da parte di soggetti non incaricati (visitatori, colleghi di altre unità organizzative) non può avvenire se non in presenza di almeno un incaricato.

Il visitatore non può accedere alle scrivanie. Dove previsto non può oltrepassare il bancone o altro dispositivo predisposto alla separazione dell'area operativa dall'area consentita al pubblico.

In caso di accesso all'area operativa da parte di visitatori eventualmente autorizzati, ad esempio tecnici, le pratiche presenti sulle scrivanie dovranno essere rese non accessibili o riposte.

Durante la presenza degli incaricati nell'area operativa i dispositivi di conservazione possono essere lasciati aperti ma vanno chiusi dall'ultimo incaricato che lasci l'area.

I dispositivi di conservazione posizionati in locali non chiusi o in aree aperte (corridoi) devono essere chiusi a chiave dopo ogni utilizzo.

I locali destinati ad uso archivio devono essere chiusi e le chiavi devono essere a disposizione nei locali operativi.

Richieste di dati per finalità organizzative (mail, telefono)

Ogni necessità di richiesta agli interessati (personale, alunni e famiglie) deve essere valutata rispetto ai dati già in possesso e, se ritenuta necessaria, deve essere formulata mediante un modulo che sia riconducibile all'Istituto e che rechi l'informativa relativa ai trattamenti per i quali è necessario fornire i dati richiesti.

Spetta al Dirigente o al Responsabile protezione dati la valutazione della necessità della richiesta di consenso. In tal caso il modulo dovrà prevedere la separazione fra l'informativa, che deve essere trattenuta dagli interessati, e il consenso, che deve restare allegato ai dati forniti come prova dell'avvenuto rilascio.

Consenso e liberatorie per utilizzo immagini con diffusione

La produzione e l'utilizzo di immagini o filmati relativi ad attività didattiche è già autorizzato al momento di consegna o messa a disposizione dell'informativa agli interessati.

Il trattamento dei file elettronici dovrà avvenire sui sistemi dell'Istituto e rispettare le regole di utilizzo previste ai punti seguenti.

Nel caso sia necessaria la diffusione delle immagini (pubblicazione sul sito web o su canali di condivisione non riservati) è necessario, volta per volta, ottenere il consenso degli interessati predisponendo un apposito modello nel quale verranno descritte le caratteristiche dell'evento e della necessità di diffusione.

In alcuni casi il modello dovrà contenere, oltre ai riferimenti alla normativa privacy, anche una liberatoria all'utilizzo delle immagini senza pretesa di compenso o di rivendicazioni di diritti di utilizzo da parte degli interessati.

Il modulo dovrà prevedere la separazione fra l'informativa, che deve essere trattenuta dagli interessati, e il consenso, che deve restare allegato ai dati forniti come prova dell'avvenuto rilascio.

Utilizzo di dispositivi personali

Benché si disponga di una pluralità di strumenti che consentono la conservazione, l'elaborazione, la condivisione di documenti, tabelle, testi contenenti informazioni o dati personali, il loro utilizzo deve essere limitato e non deve accrescere i rischi di violazione dei dati (ricordiamo che secondo il legislatore le violazioni possono riguardare: la riservatezza, la disponibilità, l'integrità).

In tale ottica agli incaricati **non è consentito l'utilizzo di dispositivi personali** (PC, notebook, netbook, tablet, smartphone, macchine fotografiche, memorie flash, drive USB, indirizzi di posta elettronica personali) per conservare, elaborare, condividere e inviare documenti contenenti dati o informazioni personali.

I documenti prodotti su dispositivi personali, o su dispositivi in dotazione nell'Istituto ma non destinati alla conservazione (PC di laboratorio, di classe, PC in aula insegnanti), e successivamente posizionati sui sistemi in dotazione all'Istituto, dovranno venire cancellati o resi in forma anonima, anche applicando il principio di pseudonimizzazione previsto dal GDPR (trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive).

In determinate condizioni di necessità, o per operazioni da effettuarsi fuori dall'ambiente di lavoro, è ammesso l'utilizzo di dispositivi personali solo per accedere a portali web o aree di condivisione, purché vengano rigidamente applicate le misure di sicurezza contenute nel capitolo "credenziali di autenticazione" e che dei documenti trattati non vengano effettuate copie sui dispositivi stessi.

In caso venga assegnato un indirizzo di posta elettronica d'Istituto, non è consentito utilizzare programmi c.d. client di posta sui propri dispositivi personali per ricevere ed inviare messaggi e allegati. L'accesso all'indirizzo di posta in dotazione dovrà avvenire esclusivamente mediante portale web.

Non è consentito l'invio di documenti in forma di allegato di posta elettronica da indirizzi personali o da indirizzi forniti dall'Istituto ma configurati su dispositivi personali. Tali invii, se necessari, devono avvenire dai sistemi dell'Istituto.

In caso di ricezione di un allegato di posta elettronica su indirizzi personali o su indirizzi forniti dall'Istituto ma configurati su dispositivi personali, l'incaricato dovrà, una volta conferito l'allegato nei sistemi dell'Istituto, cancellare il messaggio ricevuto e svuotare il cestino.

Ogni trattamento effettuato in violazione del presente capitolo espone al rischio di violazione in caso di guasto, furto o smarrimento, accesso o utilizzo da parte di terzi dei dispositivi personali.

Nel caso si verifichino uno o più degli eventi ipotizzati al punto precedente, l'incaricato deve darne immediata segnalazione al Dirigente o a Responsabile della protezione dati, fornendo tutti gli elementi necessari a valutare il contenuto violato, il tipo di violazione, le potenziali conseguenze, al fine di determinare la necessità di notifica al Garante o di comunicazione agli interessati.

Credenziali di autenticazione

Al personale e ai collaboratori dell'Istituto possono essere assegnate una o più credenziali personali di accesso per mezzo delle quali si viene autorizzati ad accedere a:

- computer,
- dispositivi mobili,
- programmi interni (sui sistemi dell'Istituto)
- portali applicativi web
    - segreteria digitale
    - registro elettronico
    - area riservata del sito web dell'Istituto
    - posta elettronica di istituto

non rientrano in questa categoria le credenziali che identificano l'Istituto su portali web privati o pubblici. Tali credenziali devono essere conosciute, di norma, da un limitato numero di incaricati, se non dai soli DS o DSGA.

La parte variabile di tali credenziali va sostituita immediatamente nel momento in cui venga meno l'incarico di un collaboratore che ne sia a conoscenza.

Caratteristiche e primo utilizzo

- Di norma la credenziale è composta da una parte fissa (nome o codice) e da una parte variabile (password o pin). Talvolta la parte fissa può essere sostituita da una tessera o badge.
- La parte variabile viene inizialmente assegnata d'ufficio e vale soltanto per il primo utilizzo. L'operatore verrà obbligato a sostituirla al primo accesso e, successivamente, ogni 90 giorni. Eventuali deroghe alla regola enunciata saranno motivate da vincoli tecnici. Di volta in volta verranno comunicate le regole sostitutive. Restano applicabili, anche se non imposte dal sistema, il cambio al primo utilizzo ed il successivo cambio almeno ogni 90 giorni. Sarà cura dell'incaricato provvedere utilizzando la funzione di "cambio password" prevista da ogni programma o piattaforma.
- Nessuno, nemmeno tecnici o amministratori di sistema o Dirigenti, ha la necessità di essere a conoscenza della credenziale di accesso personale di un incaricato. È un atto illecito e va segnalato al Responsabile protezione dati che, verificata l'eventuale necessità, disporrà a che vengano adottate misure alternative per affrontarla.
- In caso venga dimenticata la parte variabile della credenziale dovrà essere attivata la procedura di recupero password prevista dall'applicativo o dal portale. Tale procedura fornirà, secondo modalità che possono variare di volta in volta, una password temporanea che dovrà essere modificata autonomamente dall'incaricato al primo accesso.
- In caso si abbia il dubbio che le proprie credenziali siano a conoscenza di altri, dovrà essere effettuato tempestivamente il cambio della password secondo le modalità previste dal sistema al quale le credenziali consentono di accedere.

Composizione della password

- Quando la parte variabile è composta da un pin (personal identification number) le regole per l'utilizzo e la sostituzione saranno diverse di volta in volta, a seconda della natura del portale.
- In caso la parte variabile sia composta da password questa dovrà rispettare le seguenti caratteristiche:
- lunghezza minima — 8 caratteri
- complessità — presenza di almeno 3 elementi diversi fra MAIUSCOLE, minuscole, numeri 0-9, segni *!&$#?
- ripetizioni — non usare una password usata in precedenza
- facilità — non può contenere sequenze (1111 1234 abcd)
- riferimenti — NO riferimenti facilmente riconducibili all'incaricato

alcuni sistemi di autenticazione controllano la conformità della password inserita con le caratteristiche indicate. Sui sistemi che non effettuano tali controlli è responsabilità dell'incaricato rispettare le caratteristiche.

Regole di utilizzo

- Le credenziali sono personali, cioè identificano univocamente il collaboratore;
- ogni collaboratore viene autorizzato a compiere le operazioni compatibili con il proprio profilo operativo;

- ogni attività effettuata utilizzando le proprie credenziali viene tracciata ed è attribuibile all'incaricato;
- chi consente ad altri di usare le proprie credenziali gli consente di compiere operazioni con il proprio profilo e a lui riconducibili;
- al fine di prevenire l'utilizzo del proprio profilo da parte di terzi è importante:
    - non lasciare incustodito un dispositivo, un programma o un portale al quale si ha avuto accesso, senza prima salvare il proprio lavoro, quindi bloccare il dispositivo, chiudere la sessione, disconnetterlo o spegnerlo;
    - in caso di utilizzo di accesso a portali web o programmi da dispositivi ai quali accedono anche altre persone non utilizzare le funzioni di memorizzazione delle credenziali previste dai browser.

Utilizzo di social network o iscrizione a portali esterni

- Non è consentito iscriversi o registrarsi a portali, servizi gratuiti o a pagamento, servizi di posta elettronica, social network o siti di varia natura, a nome dell'Istituto o a titolo personale ma essendo identificabili con l'Istituto.
- Ogni necessità di registrazione o iscrizione deve essere motivata e richiesta al Dirigente il quale ne valuterà la pertinenza.
- Ogni registrazione o iscrizione autorizzata dovrà essere documentata e gli estremi consegnati in Segreteria. Ogni futura variazione degli estremi dovrà comportare il tempestivo aggiornamento della documentazione.
- In caso di cessata necessità di utilizzo di una registrazione ad un servizio si dovrà darne immediata comunicazione al Dirigente che provvederà alla chiusura del servizio stesso, se prevista.
- In caso di utilizzo di profili propri su portali di social network è sconsigliato richiedere o concedere "amicizia" o autorizzazione alla condivisione, a studenti o famigliari di studenti.
- In caso di utilizzo di profili istituzionali su portali di social network le regole per l'accettazione di iscrizioni o di richieste di accesso verranno di volta in volta stabilite dal Dirigente.
- Per nessun motivo è possibile richiedere direttamente allo studente il numero di telefono o l'indirizzo di posta elettronica.
- Ogni necessità di raccolta di numeri di telefono o indirizzi di posta elettronica deve essere motivata e richiesta al Dirigente il quale ne valuterà la pertinenza.
- Ogni richiesta di quanto al punto precedente, se autorizzata, dovrà essere effettuata mediante modulistica ufficiale dell'Istituto.
- L'utilizzo dei dati raccolti si intende autorizzato per le sole finalità per le quali viene richiesto.
- Ogni altro utilizzo, istituzionale o personale, costituisce una violazione della riservatezza punibile amministrativamente ai sensi della normativa italiana ed europea vigente.

Utilizzo di strumenti elettronici assegnati

- Al personale possono venire assegnati dispositivi portatili per l'accesso al sistema informatico o ai portali di gestione delle procedure, quali tablet, netbook o notebook.
- I dispositivi posso essere a disposizione, cioè per utilizzo nell'edificio scolastico e da riporre al termine, o assegnati singolarmente per un utilizzo sia all'interno dell'edificio scolastico che in altri luoghi.
- **In qualsiasi caso l'utilizzatore non è autorizzato a modificare la configurazione del dispositivo mediante installazione o rimozione di componenti, di configurazione di sistema o di software.**

- Ogni necessità di modifica va segnalata al Dirigente che provvederà alla valutazione della segnalazione ed alla eventuale autorizzazione.
- Il dispositivo deve essere spento al termine dell'utilizzo. Il dispositivo non va lasciato incustodito con le credenziali inserite. Se il sistema lo prevede è possibile disconnettere le proprie credenziali così da renderlo non accessibile anche per brevi pause.
- Il dispositivo non può essere affidato o lasciato utilizzare da altri che non siano a loro volta autorizzati e non può essere utilizzato per attività non pertinenti con il lavoro.
- Il collaboratore al quale viene assegnato o affidato un dispositivo lo dovrà accudire con la massima attenzione al fine di non compromettere il suo funzionamento.
- L'eventuale malfunzionamento di un dispositivo va segnalato tempestivamente affinché si possa procedere alla sua riparazione o alla sua sostituzione, temporanea o definitiva.
- L'eventuale perdita (furto, smarrimento) di un dispositivo va segnalata tempestivamente affinché si possa procedere alla valutazione del danno e delle conseguenze in base alla procedura c.d. Data Breach adottata dall'Istituto.