LICEO STATALE "*Enrico Fermi*" CECINA
LICEO SCIENTIFICO - LICEO SCIENTIFICO Sez. INDIRIZZO SPORTIVO - LICEO CLASSICO - LICEO LINGUISTICO
LICEO DELLE SCIENZE UMANE - LICEO DELLE SCIENZE UMANE opzione ECONOMICO SOCIALE
Via Ambrogi,12 - 57023 Cecina (Li) **- Tel**. 0586/ 681515
Email: lips02000l@istruzione.it **Pec :** lips02000l@pec.istruzione.it **Internet:** www.fermicecina.edu.it
C.F. 80009280498 C.M. LIPS02000L

Procedura per la creazione delle mail

Premessa

La presente procedura ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori etc) al fine di utilizzare i beni dell'ente ed evitare condotte inconsapevoli o scorrette che potrebbero esporre l'ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informativa, informazione correttezza nell'ambito dei rapporti di lavoro ed inoltre finalizzato a prevenire comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad esso attribuiti dall'ordinamento giuridico italiano.

A tal proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa con particolare riferimento al Regolamento UE 2016/679, alla legge 300/1970 ed ai provvedimenti emanati dall'Autorità Garante.

La presente procedura si applica ad ogni utente assegnatario di beni e risorse informatiche dell'ente ovvero utilizzatore di servizi e risorse informative dell'ente.

Più in particolare per quanto riguarda gli account di posta elettronica.

Gli account utenti vengono creati dagli amministratori di sistema (se nominati) e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso avviene tramite delle "credenziali di autenticazione" solitamente username e password, comunicate dall'amministratore di sistema (se nominato) o dal tecnico informatico a ciò appositamente autorizzato dal titolare con apposita nomina, che le genera con modalità tali da garantire la segretezza.

Le credenziali di autenticazione costituiscono dati dell'ente da mantenere strettamente riservati e non è consentito comunicare gli estremi a terzi.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno od il sospetto di un utilizzo non autorizzato del proprio account è tenuto a modificare immediatamente la password ed a segnalare la violazione all'amministratore di sistema.

Due sono i possibili scenari.

Infatti gli account se accompagnati dal nome e cognome del lavoratore anche se associati al dominio dell'ente, sono considerati in tutto e per tutto "dati personali" ai sensi dell'art. 4 del R.E. 20167679. Di conseguenza sono alla normativa sulla tutela della privacy.
Pertanto per il titolare, per evitare qualsiasi problema e sanzione, potrebbe optare per l'utilizzo di account istituzionali condivisi (es.segreteriadidattica@.....; segreteriapersonale@.....) piuttosto che quelli nominali. E questo perché in questo modo vengono eliminate tutte le problematiche relative alla riservatezza del lavoratore, non contenendo dati personali del lavoratore e non potendo così presumersi un utilizzo individuale.
Quando invece si decida di creare dei domini personali è necessario regolamentarne in maniera precisa l'utilizzo, secondo le seguenti regole.

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative.

Sono vietati comportamenti che possano arrecare danno all'Ente.

In particolare, l'utente dovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- non è consentito l'utilizzo funzioni di instant messaging a meno che autorizzate dall' area IT;
- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi nel server dell'ente) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati dall'amministratore di Sistema (se esiste)
- è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni

software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dall'ente;

- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete dell'ente qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es.tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);
- al fine di ottimizzare le risorse a disposizione della posta elettronica dell'ente e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.
- va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es.chiavi USB, dischi esterni ecc.), avvertendo immediatamente l'amministratore di Sistema (se nominato) o chiunque si occupa del sistema nel caso in cui siano rilevati virus.

L'utente, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd "Fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

L'ente, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell'amministratore di Sistema (se nominato) o del tecnico informatico, di accedere alla casella di posta elettronica dell'utente assente.
In questo caso si prevede che

- L'amministratore di Sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare con apposita nomina, può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware).

  Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività

operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

- Lo stesso Amministratore di Sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico dell'ente (ad es. rimozione di file o applicazioni pericolosi).
- L' amministratore di Sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica dell'utente per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'utente.
- L'amministratore di sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

- L'amministratore di Sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'ente per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.

In ogni caso, l'ente garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

• lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

• riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

• lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo

Particolari cautele nella predisposizione dei messaggi di posta elettronica.

Nell'utilizzo della posta elettronica ciascun utente deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti dell'ente. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione dell' ente

L'ente formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

a) conservare le comunicazioni inviate o ricevute, in particolare dalle quali si possano desumere
impegni e/o indicazioni operative provenienti dalla Committenza pubblica;

b) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:

- visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,

- una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,

- cancellare il messaggio e svuotare il "cestino" della posta,

- segnalare l'accaduto all'amministratore di Sistema (se nominato) od il tecnico informatico a ciò autorizzato dal titolare

c) evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;

d) in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica:

- adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,

- utilizzare il servizio solo per acquisire informazioni inerenti finalità dell'ente, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering,

- in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca;

e) in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;

f) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

Trasmissione e riproduzione dei documenti

Al fine di prevenire eventuali accessi ai dati dell'ente da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

• chiedere il nome del chiamante e la motivazione della richiesta;

• richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;

• verificare che il numero dichiarato corrisponda a quello del chiamante;

• procedere immediatamente a richiamare la persona che ha richiesto l'informazione, con ciò accertandosi della identità dichiarata in precedenza.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

• prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

• verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;

• nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;

• in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.