

# ***COLLEGIO ARCIVESCOVILE “CELESTINO ENDRICI”***

*Via Endrici, 23  
Trento*

## **DISCIPLINARE INTERNO PER L'UTILIZZO DI INTERNET E POSTA ELETTRONICA DA PARTE DEI DIPENDENTI**

### **1. OGGETTO**

Il presente disciplinare, adottato sulla base delle indicazioni contenute nel provvedimento generale del Garante per la protezione dei dati personali di data 1 marzo 2007, n. 13 (“**Lavoro: le linee guida del Garante per posta elettronica e internet**”, G.U. n. 58 del 10 marzo 2007) ha per oggetto i criteri e le modalità operative di accesso ed utilizzo del servizio Internet e posta elettronica da parte dei dipendenti del ***COLLEGIO ARCIVESCOVILE “CELESTINO ENDRICI”, Via Endrici, 23, Trento*** e di tutti gli altri soggetti che a vario titolo operano nella struttura.

Il ***COLLEGIO ARCIVESCOVILE “CELESTINO ENDRICI”, Via Endrici, 23, Trento***, quale titolare del trattamento dati, deve definire le modalità d'uso degli strumenti informatici dell'Ente (Internet e posta elettronica), tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali: si devono a tal proposito bilanciare gli interessi relativi alla prevenzione di usi arbitrari degli strumenti informatici, con la riservatezza dei lavoratori.

### **2. DEFINIZIONI**

Nel presente documento si intende per:

- **POSTAZIONE DI LAVORO**: personal computer, PC portatile, WBT o thin client collegato alla rete informatica dell'Ente tramite il quale l'utente accede ai servizi informatici.
- **UTENTE DI POSTA ELETTRONICA**: persona autorizzata ad accedere al servizio di posta elettronica.
- **LOG**: archivio delle attività effettuate in rete dall'utente.
- **INTERNET PROVIDER**: azienda che fornisce il canale d'accesso alla rete Internet.
- **CREDENZIALI DI AUTENTICAZIONE**: codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.
- **WHITE LIST**: elenco di siti che l'Ente ritiene comunemente attinenti all'attività lavorativa.

- BLACK LIST: elenco di siti che presentano contenuti non attinenti all'attività lavorativa e, per questa ragione, sottoposti a filtri che si attivano qualora l'utente cerchi di accedervi.

- TITOLARE DEL TRATTAMENTO: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione ed organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. (Art. 28, D. Lgs. 30 giugno 2003, n. 196).

- RESPONSABILE DEL TRATTAMENTO: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, associazione, od organismo designati facoltativamente dal titolare al trattamento dei dati personali. (Art. 29 D. Lgs. 30 giugno 2003, n. 196).

- INCARICATO: persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali. (Art. 30 D. Lgs. 30 giugno 2003, n. 196).

### **3.UTILIZZO DELLA RETE E DEL PERSONAL COMPUTER**

Le unità di rete sono aree di condivisione di dati ed informazioni strettamente legati all'attività lavorativa; pertanto i file ivi dislocati devono avere attinenza con attività e finalità di carattere istituzionale.

Ogni utente è responsabile per il proprio account e per l'uso che ne viene fatto, essendo tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso:

- Scegliere una password composta da almeno 8 caratteri alfanumerici, che non contenga riferimenti che riconducano agevolmente all'incaricato (es: non inserire nome o cognome proprio e di familiari).
- La password è personale, riservata e non può essere ceduta o comunicata ad alcuno. E' pertanto vietato l'uso della password di altri utenti; qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato e al proprio responsabile.
- E' obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta o, almeno, regolarmente ogni tre mesi.
- Per esigenze operative o di sicurezza e integrità del sistema e dei dati, l'Amministratore di sistema ha facoltà di modificare la password degli utenti.

Qualsiasi attività svolta utilizzando un codice utente e la relativa password sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. L'utente è civilmente responsabile di ogni danno cagionato all'Ente, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password.

La violazione delle presenti disposizioni può comportare l'applicazione di sanzioni disciplinari, rimanendo ferma ogni ulteriore forma di responsabilità penale.

Per evitare il pericolo di introdurre virus informatici o di alterare la stabilità delle applicazioni è vietato scaricare ed installare programmi, salva espressa autorizzazione da parte dell'Amministratore di sistema.

Non è consentito modificare le configurazioni del proprio PC.

Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni, deve darne immediata comunicazione al proprio responsabile e/o all'Amministratore di Sistema.

Il responsabile si riserva la facoltà di procedere alla rimozione di ogni applicazione o file ritenuti pericolosi per la sicurezza del sistema, non attinenti all'attività lavorativa o acquisiti ed installati in violazione del presente disciplinare.

#### **4.UTILIZZO DI PC PORTATILI**

L'utente al quale venga assegnato il PC portatile, ne è responsabile e dovrà custodirlo con la dovuta diligenza. In caso di utilizzo all'esterno dell'Ente, i PC dovranno essere custoditi in luogo sicuro.

Al PC portatile si applicano le regole sopra indicate per i PC connessi in rete, con particolare attenzione alle disposizioni concernenti i profili di accesso (password).

Sull'hard disk devono essere conservati solo i file strettamente necessari all'attività lavorativa, rimuovendo comunque, prima della restituzione del PC, quelli elaborati ed ivi salvati.

Collegarsi periodicamente alla rete interna per consentire gli aggiornamenti dell'antivirus, del sistema operativo, nonché la sincronizzazione della posta elettronica e relative cartelle pubbliche.

Non utilizzare abbonamenti Internet privati per collegarsi alla rete.

#### **5.UTILIZZO DELLA RETE INTERNET**

L'accesso ad Internet può essere effettuato da qualsiasi utente che sia autenticato (credenziali di accesso) su una qualsiasi postazione di lavoro connessa. Il lavoratore deve ricordare che Internet è uno strumento di lavoro e quindi è possibile che il datore, per ridurre i casi di utilizzo improprio del mezzo (es: visione di siti non correlati all'attività lavorativa, download di file e software, uso della rete per finalità completamente estranee alla propria mansione...), adotti misure atte ad evitare l'esercizio di un controllo a posteriori dei lavoratori.

Fra queste misure si possono enumerare: individuazione di white list (composte da soli "siti istituzionali, rispetto ai quali la navigazione è correlata e funzionale allo svolgimento della prestazione lavorativa) o black list (composte da tutti quei siti che, oltre a non avere

attinenza con il lavoro, presentano contenuti non in linea con le politiche di gestione adottate dal titolare.

L'utente è direttamente responsabile dell'uso che egli faccia del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.

Non è comunque consentito usare la rete in modo difforme da quanto previsto dal presente disciplinare, dalle leggi penali, civili ed amministrative in materia.

## **6. UTILIZZO DELLA POSTA ELETTRONICA**

Il sistema di posta elettronica attivato sulla rete dell'Ente è da intendersi strumento di lavoro e come tale deve essere utilizzato.

Viene assegnato un account di posta elettronica ad ogni utente della rete informatica, l'accesso al contenuto della quale è protetto dalla richiesta di autenticazione; inoltre, potrebbe essere creato un account condiviso fra più lavoratori; in quest'ultimo caso risulta chiara la natura non privata dello strumento e della relativa corrispondenza.

Le disposizioni di seguito riportate sono enunciate al fine di garantire un corretto utilizzo dello strumento:

- All'utente non è consentito servirsi dell'account fornito dall'Ente per l'invio di mail non connesse con l'attività professionale (es: mail a contenuto privato, giochi, appelli, petizioni, catene di S. Antonio...).
- Non è consigliato allegare al testo delle comunicazioni, materiale potenzialmente insicuro o file di dimensioni eccessive. In quest'ultimo caso utilizzare formati compressi (zip, rar...).
- Nel caso di mittenti sconosciuti o di messaggi dall'oggetto insolito, è consigliata l'eliminazione senza l'apertura del messaggio. Lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che tuttavia presentano allegati con particolari estensioni (es: .exe, .scr, .pif, .bat..).
- Nel caso in cui si debba inviare un documento all'esterno, è preferibile utilizzare un formato protetto da scrittura (es: Acrobat).
- E' consigliabile non inviare mail che contengano dati sensibili; qualora ciò sia necessario per determinate esigenze, questi devono essere inviati comunicando al richiedente un codice identificativo per ogni soggetto e trasmettendo separatamente il documento privo del nominativo dell'interessato e crittografando i file con password che dovrà essere comunicata al destinatario del messaggio per altro mezzo.
- Qualora il messaggio debba essere inviato a più soggetti, gli indirizzi vanno inseriti solo nel campo "CCn" per tutelare la riservatezza dei medesimi, che ricevono il messaggio conoscendo solamente il mittente.
- Prevedere, in caso di assenza prolungata del lavoratore (es: ferie), l'invio di messaggi di risposta automatica che indichino la durata dell'assenza ed il nominativo del soggetto al quale è possibile rivolgersi. Se l'assenza risulta imprevista (es: malattia), l'attivazione

dell'invio di messaggi automatici potrà essere richiesta dal responsabile all'Amministratore di sistema.

- L'iscrizione a mailing list è concessa solo per motivi professionali: prima di iscriversi è necessario verificare l'affidabilità del sito ed ottenere l'autorizzazione dell' Amministratore di sistema.

- L'intestatario dell'account ha facoltà di delegare ad altri il diritto d'accesso in caso di assenza prolungata e per garantire la continuità nell'attività lavorativa. Il fiduciario dovrà essere scelto e nominato fra i colleghi o i collaboratori che, qualora dovessero accedere alla casella di posta della persona assente, sono tenuti a non aprire o non considerare i messaggi che presentino contenuto non attinente alle motivazioni per cui si effettua l'accesso.

L'Amministratore di sistema o chi da esso incaricato può avere accesso all'account solo ed esclusivamente a seguito del riscontro di situazioni che abbiano pregiudicato il funzionamento del sistema.

Il paragrafo 9 del presente regolamento disciplina i profili connessi ai controlli e alle eventuali sanzioni in cui si può incorrere qualora si utilizzi tale strumento in modo difforme.

## **7. INTERRUZIONE D'UFFICIO DEL SERVIZIO**

L'Amministratore di sistema può sospendere temporaneamente il servizio di accesso ad Internet e alla posta elettronica in caso di manutenzione; l'interruzione sarà anticipatamente comunicata agli utenti, salvo casi di forza maggiore.

L'utilizzo del servizio di accesso alla Rete e all'account di posta elettronica cesserà d'ufficio nei seguenti casi:

- Qualora venga meno la condizione di dipendente o collaboratore munito di autorizzazione o se l'autorizzazione non fosse riconfermata.

- Se venga accertato un uso non corretto del servizio da parte dell'utente o estraneo ai suoi compiti professionali.

- In caso di manomissioni e/o interventi su hardware/software; diffusione o comunicazione imputabili direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni tecniche riservate; accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

- In caso di violazione o inadempimento imputabile all'utente rispetto a quanto stabilito nei precedenti punti; in ogni altro caso in cui sussista in modo evidente una violazione degli obblighi.

## **8. UTILIZZO DEL TELEFONO**

Il telefono è uno strumento di lavoro e come tale deve essere utilizzato, per fini istituzionali. Eventuali telefonate a carattere privato potranno essere effettuate con moderazione ed in casi di necessità.

## **9. CONTROLLI E SANZIONI DISCIPLINARI**

Sono interdetti al datore di lavoro controlli del personale dipendente e dei collaboratori effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970).

Ciò premesso, l'Ente può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti lavorativi che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali.

I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza.

In seguito si espongono le modalità di tali controlli:

- In prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di reparto, ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole.
- Il controllo anonimo effettuato su aree può terminare con un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando ad attenersi ai compiti e alle mansioni impartite.
- Se si dovesse ripetere l'anomalia, sarà facoltà dell'Ente procedere con controlli più mirati, anche su base individuale e successivamente procedere all'irrogazione di sanzioni disciplinari previste dall'art. 7 dello Statuto dei lavoratori (legge 300/1970), dal CCNL di riferimento ovvero dal contratto di assunzione.
- La sanzione irrogata sarà proporzionata all'infrazione e potrà consistere in un richiamo verbale, un richiamo scritto, in una multa (si regola non superiore all'importo di 3 ore di paga base), nella sospensione dal servizio e dalla retribuzione fino ad un massimo di giorni tre di effettivo lavoro.
- Nel caso in cui le infrazioni riscontrate fossero di particolare gravità (quali, ad esempio, condotte pesantemente negligenti nell'espletamento delle proprie mansioni ovvero contrarie ai principi educativi dell'Istituto e della morale cattolica), il lavoratore potrebbe incorrere nel provvedimento del licenziamento con o senza preavviso.
- In ogni caso, le eventuali infrazioni riscontrate potranno essere punite in sede disciplinare nel rigoroso rispetto di quanto stabilito dalle leggi in materia e dal CCNL di riferimento.
- Nessun provvedimento disciplinare potrà pertanto essere adottato senza la preventiva contestazione degli addebiti e senza aver sentito il dipendente a sua difesa, salvo per quanto riguarda il richiamo verbale. La contestazione degli addebiti sarà fatta mediante comunicazione scritta nella quale verrà indicato il termine entro cui il dipendente dovrà far

pervenire le proprie giustificazioni. Tale termine non potrà, in nessun caso, essere inferiore a dieci giorni dalla data di ricezione della contestazione.

- Il dipendente potrà farsi assistere dall'Organizzazione Sindacale a cui aderisce o conferisce il mandato.
- Il provvedimento disciplinare dovrà essere comunicato con lettera raccomandata inviata entro sei giorni dal termine assegnato al dipendente per presentare le proprie giustificazioni. Tale comunicazione dovrà specificare i motivi del provvedimento. Trascorso l'anzidetto periodo senza che sia stato adottato alcun provvedimento, le giustificazioni presentate dal dipendente si intendono accolte.
- I provvedimenti disciplinari comminati senza l'osservanza delle presenti disposizioni sono inefficaci.
- Non si terrà conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione.

## **10. FILE DI LOG – CONSERVAZIONE E UTILIZZO**

- I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

I file di log potranno essere utilizzati in tali casi:

- produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima;
- analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima.