Ministero dell'Istruzione dell'Università e Ricerca

C.P.I.A. 3 TORINO
Centro Provinciale Istruzione Adulti
Via Ponchielli n. 18 bis – 10024 MONCALIERI (TO)
C.F. 94071240017 - C.M. TOMM32500B
TEL. 011-6822922 – TOMM32500B@ISTRUZIONE.IT - TOMM32500B@PEC.ISTRUZIONE.IT

SEDE BRACCINI
TOCT701004
Corso Tazzoli 215/1
Torino
Tel. 011-3118386

SEDE CASTELLO MIRAFIORI
TOCT706007
Str. Castello di Mirafiori 55
Torino
Tel. 011-01133760

SEDE DI CHIERI
TOCT71000V
Via Santa Clara 8
Chieri
Tel. 011-9428480

SEDE DI MONCALIERI
TOCT71100P
Via San Matteo 14
Moncalieri
Tel. 011-6060475

SEDE I.P.M. FERRANTE APORTI
TOEE70601G
Via Berruti e Ferrero 3
Torino
Tel. 011-6194201
Fax 011-6194249

SEDE DI CARMAGNOLA
TOCT71800D
C.so Sacchirone 47
Carmagnola (TO)

C.P.I.A. 3 TORINO - -MONCALIERI
Prot. 0000146 del 10/01/2019
(Uscita)

# REGOLAMENTO INTERNO SUL CORRETTO UTILIZZO DELLA POSTAZIONE DI LAVORO, DELLA NAVIGAZIONE INTERNET E DELLA POSTA ELETTRONICA

## In conformità al D.lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016 in materia di protezione dei dati personali

***"Corretto utilizzo della postazione di lavoro, della navigazione Internet e della posta elettronica nel rapporto di lavoro"***

Questo documento è stato predisposto sulla base delle Linee guida del Garante per posta elettronica e internet pubblicate sul Registro delle deliberazioni Del. n. 13 del 1° marzo 2007, Bollettino del n. 81/marzo 2007, e dei Limiti al controllo sulla posta elettronica del dipendente del 2 aprile 2008, pubblicati sul Bollettino n. 93/aprile 2008, nonché sulla base della Direttiva N.02/09 della Presidenza del Consiglio dei Ministri-Dipartimento della Funzione Pubblica 0024438 del 26/05/2009.

Il documento è stato successivamente integrato in conformità alle previsioni del Regolamento UE 679/2016 in materia di protezione dei dati personali ("GDPR") e del D, Lgs. 196/03 e s.m.i. ("Codice" della privacy).

### ***Tutela del lavoratore***

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

***Principi generali***

Nell'impartire le prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela degli interessati.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza dei principi ex art. 5 GDPR:

- il principio di minimizzazione, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- il principio di esattezza, di integrità e riservatezza;
- il principio di liceità, correttezza e trasparenza, di limitazione delle finalità e di limitazione della conservazione, secondo cui i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime,. Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza.

In base al richiamato principio di correttezza responsabilizzazione (art. 5.2 GDPR), il titolare del trattamento è competente per il rispetto dei principi sopra elencati (ex art. 5.1 GDPR) e in grado di comprovarlo, Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e in che misura e con quali modalità vengano effettuati controlli. Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura.

In questo quadro, il datore di lavoro provvede:

- a consegnare ad ogni dipendente il presente documento informativo sugli adempimenti dell'Istituto CPIA 3 TORINO in materia di trattamento dei dati personali
- a organizzare corsi di formazione e aggiornamento sulla privacy e sull'uso corretto degli strumenti a disposizione del lavoratore

Con riguardo al principio secondo cui occorre perseguire finalità determinate, l'Istituto CPIA 3 TORINO si riserva di controllare il corretto utilizzo degli strumenti di lavoro, le cui linee guida vengono riportate nel seguente documento.

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori; in particolare non è da ritenersi consentito:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica;
- la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer affidati in uso.

L'Istituto CPIA 3 TORINO utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori,

di sistemi che consentono indirettamente un controllo a distanza, previo consenso del lavoratore stesso.

In applicazione dei principi di necessità esattezza, integrità e riservatezza l'Istituto CPIA 3 TORINO è chiamata a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.

Dal punto di vista organizzativo nella stesura del presente Regolamento è stato opportuno:

- valutare attentamente l'impatto sui diritti dei lavoratori;
- individuare preventivamente a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- determinare quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego non autorizzato.

***Corretto utilizzo della postazione di lavoro***

L'Istituto CPIA 3 TORINO, per ridurre il rischio di usi impropri delle postazioni di lavoro ha ritenuto di redigere delle linee guida al corretto utilizzo dei computer messi a disposizione dei dipendenti, secondo le norme relative alla Privacy ed alla sicurezza, che qui di seguito riportiamo:

- Ogni dipendente dell'Istituto CPIA 3 TORINO in qualsiasi funzione sanitaria e/o amministrativa svolga la propria attività è, ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003 e s.m.i., designato al trattamento dei dati, con attribuzione da parte del titolare di specifici compiti e funzioni connessi al trattamento di dati personali.
- Ogni dipendente è responsabile della custodia e dell'aggiornamento della propria login/password, nonché del PIN e del PUK relativi all'eventuale SIM CARD aziendale
- I dati personali e sensibili possono essere trattati (inseriti/modificati/cancellati) solo utilizzando i software applicativi in dotazione all'Istituto CPIA 3 TORINO e per finalità attinenti l'attività lavorativa svolta.
- La postazione di lavoro non deve essere lasciata incustodita senza disconnettersi dalla rete.
- L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro (PC-Notebook) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso, ed è quindi tenuto a:
    - Accertarsi di aver chiuso tutti i documenti aperti: per permettere ai colleghi di utilizzare lo stesso documento se condiviso su server di rete.
    - Accertarsi di aver chiuso ogni software il cui accesso è regolato da login/password o bloccare il sistema / attivare la funzione di disconnessione:
    - Ove prevista la possibilità esplicita di bloccare il sistema, l'utente deve utilizzarla (ad es. sui sistemi Windows con la combinazione di tasti CRTL + ALT + CANC e quindi "Blocca computer");
- I dati di interesse lavorativo non devono essere memorizzati sul disco fisso locale della postazione di lavoro, ma deve essere utilizzata l'area condivisa o riservata predisposta sui server dedicati. Nel caso in cui tale suggerimento non fosse seguito, è responsabilità dell'utente predisporre opportune misure di sicurezza per il salvataggio dei dati e provvedere quanto prima all'archiviazione su server.

**Si ricorda che il desktop è da considerarsi parte del disco fisso locale e pertanto non protetto da backup.**

- I dati di interesse lavorativo considerati di uso personale ed esclusivo dell'utente devono essere memorizzati nella cartella personale riservata all'utente; in nessun caso devono essere memorizzati dati sul disco fìsso locale della postazione di lavoro.
- I dati personali comuni e sensibili non devono essere archiviati su dispositivi rimovibili (CD, pen drive ecc.) né essere archiviati su supporti e/o dispositivi che non siano di proprietà dell'Istituto CPIA 3 TORINO, fatti salvi casi particolari autorizzati dalla stessa.
- Nuovi software non devono essere installati sul Personal Computer senza l'autorizzazione e la conseguente registrazione della licenza software da parte dell'amministratore di rete designato dall' Istituto CPIA 3 TORINO.

***Internet: la navigazione web***

L'Istituto CPIA 3 TORINO , per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti , upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa), invita i propri dipendenti ad autoregolamentarsi nella navigazione in Internet specialmente nella categorie sotto indicate adottando, inoltre, opportune misure che possono, così, prevenire controlli successivi sul lavoratore. In particolare:

- L'Istituto CPIA 3 TORINO si riserva di bloccare l'accesso a siti "a rischio" attraverso l'implementazione di Blacklist (elenco di siti non attinenti alla propria attività lavorativa) internazionali in continuo aggiornamento e di predisporre filtri tali da prevenire determinate operazioni/attività,
- il download dì file o software aventi particolari caratteristiche, quali file musicali o che violino in qualunque modo la normativa vigente in materia di copyright e diritto d'autore, non è consentito; anche il download di programmi che necessitano di installazione sulla postazione di lavoro, non è consentito, se non con il supporto dell'amministratore di rete designato dall'Istituto CPIA 3 TORINO è ammessa solo la navigazione in siti considerati correlati con la propria prestazione lavorativa,
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames)..
- durante la navigazione Internet vengono memorizzate alcune informazioni, qui elencate, a cui possono accedere solo l'amministratore di rete designato dall'Istituto CPIA 3 TORINO. e, su richiesta, l'Autorità Giudiziaria:
    I. indirizzi IP del computer che ha navigato
    II. sessione di navigazione dell'utente
    III. URL del sito navigato
    IV. Data e ora di inizio e fine navigazione
- il Titolare del trattamento, su richiesta dell'Autorità Giudiziaria o su indicazione motivata per iscritto di un designato al trattamento dei dati qualora constati che la navigazione Internet è utilizzata indebitamente, informate laddove presenti le Organizzazioni Sindacali, può richiedere all'Amministratore di sistema il controllo a posteriori di accessi avvenuti da una specifica stazione di lavoro in un arco temporale prefissato

- il Titolare del trattamento può fare richiesta, motivata da esigenze di servizio, all'Amministratore di sistema designato, di attuare delle politiche di restrizione di accesso ad Internet o semplicemente inibire la navigazione Internet da alcune postazioni specifiche situate in posizioni strategiche a cui l'accesso è condiviso da molti dipendenti.

***Posta elettronica***

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza. Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione o ne faccia un uso personale pur operando in una struttura lavorativa.

Risulta quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In conformità alle disposizioni vigenti in materia di protezione dei dati personali, in particolare ai principi di cui all'art. 5 del Regolamento UE 679/2016 e ai diritti dell'interessato e ai doveri del Titolare del Trattamento di cui all'art. 17 del Regolamento UE 679/2016; in riferimento alle prescrizioni di cui alle linee guida del Garante per la Protezione dei Dati personali per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007) con Delibera n. 13 del 1° marzo 2007, ai Provvedimenti del Garante per la Protezione dei Dati personali n. 551 del 27 novembre 2014 e n. 456 del 30 luglio 2015, l'Istituto CPIA 3 TORINO ha ritenuto opportuno:

- rendere disponibili indirizzi di posta elettronica ai lavoratori per finalità di servizio;
- disporre per tutti i possessori di casella postale dell'Istituto CPIA 3 TORINO:
  - che l'invio di dati personali e/o sensibili propri o di terzi, attraverso la posta elettronica, è proibito per motivi di sicurezza e che l'Ente non può quindi ritenersi responsabile della perdita di tali dati o del recapito non corretto di tali dati
  - che, osservando il principio di pertinenza e non eccedenza, l'uso prevalente della casella postale dell'Istituto CPIA 3 TORINO deve essere relativo a scopi lavorativi e che lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti, che esuli dagli scopi lavorativi, deve essere assolutamente limitato nel tempo e nella quantità
  - l'inserimento automatico della seguente informativa, in calce a tutti i messaggi di posta elettronica che vengono inviati dall'Istituto CPIA 3 TORINO.

**INFORMATIVA ex art. 13 *Regolamento* UE 679/2016 (PRIVACY)**

Le informazioni contenute nella presente comunicazione e relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o all'ente sopraindicati. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita ai sensi dell'art. 616 c.p. sia ai sensi del Regolamento UE 679/2016 e del D.Lgs. 196/03 e s.m.i. Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di informarci immediatamente inviandoci un messaggio al presente indirizzo mail.

Per maggiori dettagli consultare l'informativa completa pubblicata sul sito internet istituzionale.

***Cessazione della mailbox e dell'accesso ad internet.***

A fronte di una comunicazione degli uffici competenti all'amministratore di sistema di cessato rapporto lavorativo verranno intraprese le seguenti azioni, salvo accordi diversi con l'utenza sui tempi di cessazione:

I. Sospensione della password di accesso alla rete informatica (e conseguentemente ad Internet) con effetto alla data di cessazione del rapporto.

II. l'Ente è tenuto a disattivare l'indirizzo di posta elettronica in oggetto entro il termine di trenta giorni dalla comunicazione all'utente, secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server aziendali, con contestuale utilizzo di un risponditore automatico che avvisi gli utenti dell'avvenuta disattivazione nei trenta giorni successivi a quest'ultima, indicando altresì un indirizzo di posta elettronica aziendale alternativo cui inviare i messaggi attinenti l'attività svolta dall'azienda.

III. l'Ente è tenuto di consentire all'ex dipendente o a persona di fiducia del medesimo appositamente delegata, entro il medesimo termine quale ulteriore misura necessaria a tutela dei diritti dell'interessato ai sensi degli articoli 15, 16, 17, 18, 19, 20 e 21 del Regolamento UE 679/2016, di accedere presso la sede dell'azienda, inoltrando richiesta presso la sede legale dell'Ente a mezzo di raccomandata A/R, al contenuto dei messaggi indirizzati alla predetta casella di posta dalla data di dimissioni (licenziamento), sino all'effettiva disattivazione della casella medesima e ad ottenere una copia informatica dei dati personali che lo riguardano contenuti nella corrispondenza in tal modo conservata e ciò, a garanzia della corretta esecuzione dell'accesso medesimo, in presenza dell'amministratore di sistema o di personale di fiducia appositamente incaricato dall'Ente, nonché di provvedere, terminate le operazioni di accesso, alla cancellazione dei predetti messaggi di posta elettronica di carattere personale dell'interessato o comunque non aventi alcuna attinenza con l'attività lavorativa svolta.

IV. i dati relativi all'account di posta elettronica disattivato saranno conservati dall'Ente per un successivo periodo di anni 10 in relazione all'eventuale indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; tali dati saranno protetti con la tecnica della criptazione, e non saranno utilizzati per ulteriori finalità salvo quella menzionata. Al termine del periodo di conservazione, i dati saranno definitivamente cancellati.

V. Trascorso il mese indicato al punto I, le credenziali di accesso alla rete informatica vengono definitivamente cancellate. I files contenuti nelle cartelle personali vengono totalmente eliminati, mentre i files presenti sulle aree condivise vengono riattribuiti al personale di riferimento.

**Dichiaro di aver preso visione del REGOLAMENTO INTERNO SUL CORRETTO UTILIZZO DELLA POSTAZIONE DI LAVORO, DELLA NAVIGAZIONE INTERNET E DELLA POSTA ELETTRONICA (In conformità al D.lgs. 196/2003 e s.m.i. e al Regolamento UE 679/2016 in materia di protezione dei dati personali)**

Firma utente

*(Il presente documento è stato consegnato al personale autorizzato al trattamento dei dati che ne ha sottoscritto copia conservata nel fascicolo personale)*