

REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

INDICE

CAPO I – I PRINCIPI	2
1. SCOPO	2
2. APPLICABILITÀ	2
o Riservatezza: prevenzione contro l'accesso non autorizzato ai dati personali;	2
o Integrità: i dati personali non devono alterabili da incidenti o abusi;	2
o Disponibilità: il sistema deve essere protetto da interruzioni impreviste.	2
3. TERMINI E DEFINIZIONI	2
4. TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE	3
5. RESPONSABILITÀ PERSONALE DELL'UTENTE	3
CAPO II – MISURE ORGANIZZATIVE	4
6. AMMINISTRATORI DEL SISTEMA.....	4
7. ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD	4
Creazione e gestione degli Account	4
Gestione e utilizzo delle password	5
Cessazione degli Account	5
8. POSTAZIONI DI LAVORO	5
CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI.....	6
9. PERSONAL COMPUTER, COMPUTER PORTATILI	6
10. SOFTWARE	6
11. DISPOSITIVI DI MEMORIA PORTATILI	7
12. STAMPANTI, FOTOCOPIATRICI E FAX	7
13. GESTIONE UTILIZZO DELLA RETE INTERNET	7
14. GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE	8
Principi guida	8
Cessazione dell'indirizzo di posta elettronica aziendale	9
CAPO III – DOCUMENTAZIONE CARTACEA	9
15. CUSTODIA DEI DOCUMENTI CARTACEI	9
16. INFORMATIVA EX ART. 13 GDPR AGLI UTENTI	11
17. COMUNICAZIONI.....	11
18. APPROVAZIONE DEL REGOLAMENTO	11

CAPO I – I PRINCIPI

1. SCOPO

Lo scopo del presente disciplinare interno (di seguito anche solo il “Regolamento” è di definire l’ambito di applicazione, le modalità e le norme sull’utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre la ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI MASSA CARRARA (di seguito anche solo la “Ordine”) a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L’insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l’Ordine ai principi di diligenza, informazione e correttezza nell’ambito dei rapporti di lavoro, con l’ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall’ordinamento giuridico italiano.

A tal fine, pertanto, si rileva che gli eventuali controlli ivi 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) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – di seguito anche solo GDPR), alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D.lgs. 14 settembre 2015, n. 151 ed ai provvedimenti appositamente emanati dall’Autorità Garante (si veda in particolare Provv. 1° marzo 2007 oggi vigente).

2. APPLICABILITÀ

La presente procedura si applica a tutto il personale dipendente dell’Ordine nonché al personale esterno assegnatario di beni, risorse informatiche e di risorse a supporto alla gestione cartacea dei dati aziendali ovvero utilizzatore di servizi e risorse informative e non di pertinenza della Ordine in ambito di trattamento dei dati personali.

Il presente documento indica le norme generali e di buon senso per il corretto impiego delle informazioni presenti – a qualsiasi titolo – all’interno dell’ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI MASSA CARRARA si tratta cioè di un insieme basilare - pertanto non esaustivo - di norme comportamentali e regole pratiche atte a prevenire danneggiamento, distruzione, alterazione o perdita di accessibilità ai dati aziendali.

Con il termine "sicurezza" ci si riferisce a tre aspetti distinti:

- **Riservatezza:** prevenzione contro l’accesso non autorizzato ai dati personali;
- **Integrità:** i dati personali non devono alterabili da incidenti o abusi;
- **Disponibilità:** il sistema deve essere protetto da interruzioni impreviste.

3. TERMINI E DEFINIZIONI

- Chat: servizio offerto da Internet, che mediante apposito software permette a più interlocutori di conversare scambiandosi messaggi scritti che appaiono in tempo reale sul monitor di ciascuno;
- Client: personal computer collegato in rete a un altro computer (server), sul quale risiedono i dati che il primo utilizza;
- Computer portatile: elaboratore elettronico aziendale trasportabile con facilità;
- E-mail: messaggio inviato tramite posta elettronica;
- L’Ordine: l’organizzazione e/o comunque il Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.
- Estensione: set di tre lettere che segue il nome di un file di un computer e ne identifica il genere;
- Log: registrazione ufficiale di eventi;
- Password: parola o sigla di riconoscimento fornita dall’utente al computer per poter accedere a un sistema operativo a un programma o a un file;

- Peer to peer: sistema di computer collegati gli uni agli altri senza la connessione ad un server;
- Personal Computer: elaboratore elettronico destinato all'uso aziendale;
- Phishing: l'attività criminale di mandare e-mail o costituire un sito web al fine di ingannare qualcuno e carpire informazioni (es. numeri di carta di credito o password).
- Rete Aziendale: sistema di trasmissione delle informazioni costituito da linee di collegamento e da stazioni che possono essere costituite da elaboratori, terminali o unità di memoria;
- Server: computer collegato in rete ad altri computer (client), sul quale risiedono i dati che questi utilizzano;
- Smartphone: apparecchio elettronico che combina le funzioni di un telefono cellulare e di un computer palmare.
- Spamming: mandare messaggi a diverse persone tramite e-mail o internet generalmente a fini commerciali;
- Tablet: elaboratore elettronico aziendale compatto con interfaccia touch;
- Utente: colui che si serve di un'attrezzatura di lavoro.

4. TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE

I beni fisici e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'Ordine.

Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ordine), e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ordine, sarà dalla stessa considerata come avente natura aziendale e non riservata.

5. RESPONSABILITÀ PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ordine nonché dei relativi dati trattati per finalità aziendali.

A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ordine, è tenuto a tutelare (per quanto di propria competenza) il patrimonio pubblico da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.

Ogni Utente, pertanto, è tenuto, in relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento.

Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Ordine e quindi alla Pubblica Amministrazione.

ADEMPIMENTI GENERALI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dall'Ordine, atte a salvaguardare la riservatezza e l'integrità dei dati;

- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

CAPO II – MISURE ORGANIZZATIVE

6. AMMINISTRATORI DEL SISTEMA

L'Ordine conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche aziendali. I principali compiti, a titolo meramente esemplificativo e non esaustivo sono:

- 1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ordine;
- 2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- 3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- 4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
- 5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
- 6) provvedere alla sicurezza informatica dei sistemi informativi aziendali, nel rispetto di quanto prescritto dal GDPR;
- 7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso.
- 8) Gli AdS dell'Ordine sono esterni all'ente.

7. ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali, per singola postazione lavorativa.

La gestione di tali account segue quanto sotto espressamente previsto:

- l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza;

- le credenziali di autenticazioni costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi;
- se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al personale IT di riferimento;
- ogni Utente è responsabile dell'utilizzo del proprio account Utente;
- in base a quanto previsto dalla legge, in caso di assenza improvvisa o prolungata del lavoratore (o Utente) e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza ed operatività delle risorse informatiche dell'Ordine, la stessa si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente è tenuto a modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 90 giorni conformemente a quanto previsto.

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.);
- utilizzare almeno tre delle seguenti categorie: un carattere maiuscolo, un carattere minuscolo, un numero, un carattere non alfanumerico tipo "@#\$\$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone aziendale) non è conforme alla normativa e costituisce violazione del presente Regolamento.

Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 15 giorni previa comunicazione da parte dell'ufficio del personale.

Qualora vi sia richiesta di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'amministratore di sistema procederà a riassegnare una nuova password temporanea al fine di consentire all'utente l'accesso ai sistemi presso cui è accreditato, è obbligatorio che l'utente modifichi la password fornita dall'ADS subito dopo il primo accesso.

8. POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *device* concesso dall'Ordine in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni, l'Ordine ha adottato le regole tecniche, che di seguito si riportano:

- ogni PC, notebook (accessori e periferiche incluse), e altro *device*, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ordine, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- è dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;

- il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ordine. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa autorizzazione dell'Ordine;
- le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
- Costituisce buona regola la pulizia periodica (almeno ogni tre mesi) degli archivi e del desktop del proprio PC, con cancellazione dei file obsoleti o inutili, in particolare deve essere prestata attenzione alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante;
- L'utente è tenuto a scollegarsi dal sistema/rete ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (es. blocco del PC con CTRL+ALT+CANC/LOGO WINDOWS+L, screen-saver con password, ecc.) al fine di evitare che persone estranee effettuino accessi non permessi. Il PC deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al Titolare eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
- l'Ordine si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

9. PERSONAL COMPUTER, COMPUTER PORTATILI

Il personal computer, il computer portatile presente sul proprio posto di lavoro o assegnato sono considerati quali strumenti di lavoro di proprietà della Ordine, e devono essere utilizzati per compiere mansioni lavorative.

Ne consegue che gli utenti sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione dell'Ordine;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ordine;
- è onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro.

Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali *file* elaborati prima della sua riconsegna.

Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, l'Ordine in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati.

10. SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Ordine per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").

L'Ordine richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software in azienda:

- l'Ordine acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;
- non è consentito fare né il download né l'upload tramite internet di software non autorizzato;
- l'Ordine, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;
- l'Ordine non tollererà la duplicazione illegale del software.

11. DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, etc.

L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali per lo scambio dati, se non preventivamente autorizzati per iscritto dall'Ordine;

- è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto.

Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Ordine, i dispositivi saranno soggetti (ove compatibili) al presente Regolamento.

12. STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte della Ordine.

È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

13. GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dall'Ordine, alla navigazione Internet. Con il presente Regolamento si richiama gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ordine stessa.

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- a. l'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- b. non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, ad esclusione delle operazioni / casi espressamente autorizzati dall'Ordine e rientranti nell'attività lavorativa dell'Utente;
- c. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- d. non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames);
- e. non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- f. è consentito l'utilizzo di soluzioni di Instant Messenger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ordine previa autorizzazione della direzione di riferimento;
- g. non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- h. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;
- i. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ordine in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nocivo all'immagine dell'Ordine.

Per facilitare il rispetto delle predette regole, l'Ordine si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).

L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza.

14. GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Principi guida

Ad ogni Utente titolare di un account, l'Ordine provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà dell'Ordine ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate per la ricezione dei messaggi, mentre per le risposte o gli invii, è consigliabile utilizzare la casella di posta individuale assegnata.

Attraverso l'e-mail aziendale, gli utenti rappresentano pubblicamente l'Ordine e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti.

- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus).
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
- rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

L'utente che riceve una e-mail a carattere, violento, razzista o pornografico, o che rappresenti forme di spamming o phishing ha il dovere di avvertire rapidamente l'Ordine affinché siano prese le misure necessarie per fermare il ricevimento di questi messaggi non sollecitati. È vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato.

Non è consentito agli utenti, al contrario:

- diffondere intenzionalmente e senza autorizzazione il proprio indirizzo e-mail aziendale attraverso la rete internet;
- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (es: presentazioni o materiali video aziendali).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".

Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

In ogni caso è fatto divieto all'Utente di collegarsi, anche attraverso servizi *webmail*, al proprio account di posta elettronica aziendale mediante telefono cellulare/smartphone personali.

Si ricorda che l'utilizzo di caselle di posta elettronica personale per scopi lavorativi è assolutamente vietata.

Rispetto all'utilizzo della posta elettronica certificata si applicano, ove compatibili, le presenti disposizioni.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato a partire da 15 giorni successivi di cessazione previa comunicazione da parte dell'ufficio del personale; si disporrà la definitiva e totale cancellazione dello stesso entro 6 mesi dall'interruzione del rapporto di lavoro previa comunicazione da parte dell'ufficio del personale. In ogni caso, l'Ordine si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

CAPO III – DOCUMENTAZIONE CARTACEA

15. CUSTODIA DEI DOCUMENTI CARTACEI

I documenti trattati dovranno essere soltanto quelli pertinenti con la propria mansione aziendale, in base alle indicazioni impartite dal proprio responsabile ed alle linee guida generali ricevute nella propria lettera di incarico.

TRATTATE E ARCHIVIALE CON CURA I DOCUMENTI

Gestione dell'archiviazione dei documenti

I dati cartacei devono essere conservati in faldoni, raccoglitori e cartelline non trasparenti riposti negli appositi armadi, ove necessario muniti di ante con serratura, sugli scaffali e sulle scrivanie.

I documenti contenenti dati sensibili devono essere conservati in armadi chiusi a chiave, o – in alternativa – negli archivi che in azienda sono ad accesso selezionato e controllato.

Manipolazione dei documenti

Occorre ridurre al minimo la permanenza di documenti sulle proprie scrivanie (come sopra descritto). In alcuni casi non è permesso il mantenimento dei documenti a vista sulle scrivanie. Nel caso di spostamenti in azienda con documenti in mano, impiegare sempre una cartellina o un raccoglitore non trasparenti. Qualora si abbandona la propria postazione di lavoro si deve chiudere la porta a chiave e se ciò non è possibile, si deve riporre i documenti nella cassettera custodita.

Gestione di stampe, fotocopie e fax

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

Smaltimento/distruzione di documenti e copie

I documenti riservati che non servono più vanno opportunamente distrutti, e non cestinati.

Copie e trascrizioni non autorizzate

Se non si è autorizzati, ed in tutti i casi in cui non è strettamente necessario, non effettuare fotocopie o trascrizioni di stampe, tabulati, elenchi, rubriche e di ogni altro materiale.

Inoltre, per i documenti di livello con riservatezza medio e/o alto, non consegnare mai a persone non autorizzate stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

CHIAVI

Le modalità di accesso e di utilizzo delle chiavi degli uffici, degli archivi e degli armadi provvisti di chiavi sono stabilite dai rispettivi responsabili di funzione che provvedono, a loro discrezione, a comunicarle, anche verbalmente, a tutti o solo a qualcuno degli incaricati.

SICUREZZA E PREVENZIONE

Rispettare sempre tutte le norme di sicurezza e prevenzione previste dalle procedure di sicurezza dell'azienda ORDINE DELLE PROFESSIONI INFERMIERISTICHE DI MASSA CARRARA.

ADEMPIMENTI

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- casseti e armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;

- l'accesso fuori orario lavorativo a documenti contenenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate (anche verbalmente, sempre sotto la responsabilità degli incaricati).
- è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

16. INFORMATIVA EX ART. 13 GDPR AGLI UTENTI

Si rimanda all'informativa dipendenti rilasciata a norma dell'art. 13 del GDPR per conoscere nel dettaglio la tipologia di trattamento posto in essere con riferimento agli strumenti adottati dall'Ordine nel rispetto delle normative di settore.

17. COMUNICAZIONI

Il presente Regolamento è messo a disposizione degli utenti, per la consultazione, al momento dell'assegnazione di un account Utente.

Ad ogni aggiornamento del presente documento, ne sarà data comunicazione tramite l'invio di apposito messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente Regolamento.

Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Ordine per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es: e-mail).

18. APPROVAZIONE DEL REGOLAMENTO

Il presente Regolamento è stato approvato dal CONSIGLIO DIRETTIVO dell'Ordine in data 22/04/2025.

Massa Carrara, li 22/04/2025.

L'Ordine, in persona del Presidente Dott. Luca Fialdini