ORDINE
DEGLI AVVOCATI
DI PESARO

REGOLAMENTO SULLA SICUREZZA E L'USO DEGLI STRUMENTI INFORMATICI

Premessa generale

Il presente documento contiene le disposizioni, le misure organizzative e comportamentali che i dipendenti, i collaboratori a qualsiasi titolo dell'Ordine e gli utenti sono chiamati ad osservare per contrastare i rischi informatici.
Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione dal COA di Pesaro deve sempre ispirarsi al principio della diligenza e correttezza, con il presente Regolamento s'intende contribuire alla massima diffusione della cultura della sicurezza, per evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici e nel trattamento dei dati.
Il Regolamento è dettato e va interpretato e applicato nel rispetto:

- della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- del Regolamento Europeo 679/16 "General Data Protection Regulation"; in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- dell'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

Pubblicazione

Al presente documento e ai suoi futuri aggiornamenti viene data diffusione attraverso la sua pubblicazione sul sito istituzionale dell'Ordine, l'affissione nei locali dell'Ordine e la comunicazione al personale dipendente dell'Ordine e di Fondazione Forense.
Ogni dipendente e collaboratore è tenuto a rispettare il presente Regolamento e deve sottoscriverlo per accettazione di ogni norma in esso contenuta.

INDICE

Premessa

Il presente regolamento definisce le condizioni di utilizzo del Sistema Informatico da parte dei dipendenti, collaboratori e utenti del COA di Pesaro attraverso gli strumenti messi a disposizione dall'Ordine, per l'efficace svolgimento delle attività proprie dell'amministrazione e dei servizi ad esse correlati.

Il S.I. risponde a usi e obiettivi pubblici e l'operatore che lo utilizza deve orientare il suo comportamento al perseguimento di tali scopi. L'utilizzo del Sistema è monitorato nel rispetto della normativa sulla privacy e delle norme a tutela del lavoratore. Il Presente regolamento prevede altresì un sistema sanzionatorio collegato all'uso improprio delle strumentazioni informatiche.

Tutti gli apparati che l'Ordine mette a disposizione degli utenti indicati nelle premesse generali per lo svolgimento dell'attività lavorativa o istituzionale devono essere utilizzati da parte di coloro che vi operano, a qualunque livello e con qualsiasi rapporto, in conformità ai principi espressi dal Codice di comportamento dei dipendenti pubblici D.P.R. n. 62 del 2013, nonché dal Codice di comportamento dei dipendenti dell'Ordine degli Avvocati di Pesaro, quando adottato.

1) Principi generali

L'utilizzo degli strumenti informatici è concesso unicamente per finalità strettamente pertinenti all'attività lavorativa e istituzionale in maniera lecita, appropriata, efficiente e razionale e deve altresì rispettare i principi etici e di correttezza e i doveri stabiliti nei sopracitati Codici di comportamento, nonché la privacy e la riservatezza/segretezza dei dati, trattati secondo le normative vigenti.
In linea con quanto indicato dal Dipartimento della Funzione Pubblica (Direttiva n. 02/09), il presente regolamento disciplina le modalità e finalità di utilizzo della strumentazione informatica, nonché le modalità di controllo di tale utilizzo, per garantire, nel rispetto della dignità e riservatezza delle persone in coerenza anche con la normativa vigente in materia di protezione dei dati personali (Regolamento (UE) 2016/679 - D.Lgs.n.196/2003) e con quanto prescritto dal Garante per la protezione dei dati personali con la delibera n.13 del 1 marzo 2007, la sicurezza dei dati e del sistema informatico aziendale.

2) Destinatari

Sono destinatari del presente Regolamento tutti i collaboratori del COA con rapporto di lavoro subordinato (di qualsiasi tipologia) e coloro che svolgano, a qualsiasi titolo, attività per conto del COA di Pesaro o comunque accedano al sistema informatico di quest'ultimo (es. dipendenti di Fondazione Forense, Mediatori, componenti e iscritti all'O.C.C. di Pesaro).

3) Modalità di utilizzo della strumentazione informatica

I destinatari di cui al punto 2) si impegnano ad utilizzare la strumentazione informatica nel rispetto dei principi di cui al precedente punto 1) e a osservare le seguenti norme comportamentali:

3.1 Utilizzo di Internet

L'accesso alla rete Internet è consentito principalmente per scopi di studio, ricerca e per l'accesso a dati ed informazioni concernenti l'attività istituzionale; l'accesso per motivi personali è consentito soltanto in caso di necessità e comunque non in modo ripetuto o per periodi di tempo prolungati, evitando di:

a. accedere a siti e/o acquisire e/o diffondere contenuti informativi lesivi dell'onorabilità individuale

o collettiva o altro materiale potenzialmente offensivo o diffamatorio.
b. partecipare a social network (Facebook, Twitter e simili), Blog o Forum di discussione, salvo quanto direttamente collegato ad attività rientranti nell'ambito della comunicazione esterna istituzionale;
c. rimanere collegati per periodi di tempo prolungati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, perché ciò può appesantire il traffico della rete;
d. scaricare programmi, anche gratuiti non indispensabili allo svolgimento dell'attività lavorativa, in ogni caso segnalandolo preventivamente al proprio responsabile o all'assistenza informatica;
e. accedere a servizi con finalità ludiche o a chat line;
f. accedere a siti per la condivisione e lo streaming di contenuti multimediali e simili, a meno che non si tratti di siti riconducibili all'attività lavorativa.

3.2 Utilizzo del PC

Non è consentito all'utente modificare le caratteristiche e le impostazioni di sistema del proprio PC.

Non è consentito all'utente di archiviare files sul Desktop del proprio PC: poiché il Desktop è una cartella di sistema, in caso di malfunzionamento e necessità di reinstallazione del sistema operativo tutti i files memorizzati andrebbero persi.
Ostano, inoltre, a tale procedura, evidenti ragioni di tutela della privacy dei dati trattati.
È consentita la provvisoria archiviazione sul Desktop di brochures pubblicitarie in formato .pdf, che siano pervenute all'Ordine e abbiano pertinenza con l'attività istituzionale.

In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, l'utente deve provvedere a proteggere il proprio computer attraverso la sospensione o il blocco della sessione di lavoro, riattivabile a mezzo password.
Al termine dell'orario di servizio, prima di lasciare gli uffici, deve assicurarsi di avere opportunamente spento il proprio PC.

L'utente è responsabile del PC portatile e degli eventuali accessori a lui assegnati e deve custodirli con diligenza, sia all'interno degli uffici, sia durante gli spostamenti esterni, fino alla loro riconsegna. Particolare attenzione deve essere prestata nell'utilizzo e nella custodia del PC portatile al di fuori della rete e degli uffici dell'Ordine (es. per smart working e telelavoro) nella connessione a reti esterne e nella rimozione di eventuali file personali memorizzati nel medesimo prima della riconsegna.

3.3 Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti digitali ecc. …) è riservato esclusivamente all'attività lavorativa. Devono essere evitati sprechi o utilizzi eccessivi.

4) Sicurezza e Privacy

4.1 Strumentazioni informatiche

Nell'utilizzo delle strumentazioni informatiche occorre adottare le seguenti cautele:

a. mantenere segrete le proprie credenziali di autenticazione (password), sia quelle d'accesso alla strumentazione in dotazione sia quelle d'accesso ai vari programmi utilizzati nell'ambito della propria attività lavorativa. Dette credenziali vanno conservate con massima diligenza e in nessun caso devono essere annotate su supporti accessibili al pubblico e tanto meno vanno lasciate in vista (es.

assolutamente deprecabile: su post-it attaccati al PC);
b. non cedere, una volta autenticati nel proprio PC, l'uso della propria postazione a persone non autorizzate, in particolare per l'accesso a Internet e ai servizi di posta elettronica;
c. adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la sicurezza dei dati trattati e dei dati che possono fornire indicazioni utilizzabili per eventuali intrusioni nel S.I.;
d. utilizzare, in caso di trattamento di dati personali, le cartelle di rete, su Cloud o i supporti di memorizzazione messi a disposizione dall'Ordine al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali;
e. prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server);
f. non connettere alla rete interna apparati esterni (es. modem o router) che possano compromettere il corretto funzionamento della rete;
g. non utilizzare strumenti di messaggistica istantanea (per es. Skype, Messenger, WhatsApp) per motivi personali;
h. non introdurre o diffondere nella rete aziendale programmi illeciti (es. virus, spyware, ecc.);
i. non compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;
j. non rimuovere il programma antivirus installato sulla postazione di lavoro;
k. verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili;
l. nel caso in cui il software antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento all'assistenza informatica; non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti;
m. utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Ordine; l'installazione di eventuali software aggiuntivi dovrà essere previamente autorizzata;
n. non salvare i dati all'esterno e non utilizzare dispositivi di memorizzazione (pennette usb, dischi esterni, masterizzatori, ecc.), se non previa autorizzazione espressa del COA;
o. non lasciare incustoditi i dispositivi mobili, come tablet e notebook;
p. in caso di incidente di sicurezza (come ad esempio nei casi di accesso non autorizzato o di minacce informatiche al sistema), attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi.

4.2 Posta elettronica

La casella di posta eventualmente assegnata dall'Ordine all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
L'eventuale "personalizzazione" dell'indirizzo con indicazione di nome o cognome dell'utente non comporta il suo carattere privato, in quanto si tratta di strumenti di esclusiva proprietà dell'Ordine, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Nei messaggi inviati tramite posta elettronica da dominio istituzionale sarà accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente*".

Nell'utilizzo della posta elettronica occorre adottare le seguenti cautele:

a. utilizzare la posta elettronica messa a disposizione dall'ente per lo svolgimento dell'attività

lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
b. non utilizzare mail esterne in software di posta elettronica (es. Outlook Express, Thunderbird), in quanto le stesse comportano rischi per la sicurezza dei sistemi; è consentito - con moderazione - l'utilizzo a fini privati di mail esterne via web (es. Google Mail);
c. è obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare non si devono aprire allegati a messaggi email dal mittente e/o dall'oggetto sospetti o di formato tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.; ciò per prevenire i rischi causati da software nocivi (per es. virus, spyware, cryptolocker, ecc.);
d. nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, è rigorosamente vietato archiviare o copiare gli allegati, anche se provvisoriamente, sul desktop del proprio PC. I files da allegare dovranno essere di volta in volta recuperati dalla relativa cartella di archiviazione e prima d'inviare la email dovrà esserne verificata la pertinenza rispetto alla comunicazione e la qualifica del destinatario a riceverli.
e. limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail istituzionale su siti web pubblici (per es. forum, mailing list, ecc.);
f. nell'utilizzo della posta elettronica certificata, le credenziali (user id e password) per accedere a tale casella di posta devono essere a conoscenza unicamente dei collaboratori dell'ufficio autorizzati dal responsabile del servizio;
g. è vietato l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione. Durante i periodi di assenza dei dipendenti (es. ferie, malattia, infortunio) il COA autorizzerà il titolare della casella di posta a designare (o designerà direttamente) un altro dipendente, per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli rilevanti per lo svolgimento dell'attività lavorativa;
h. per imprescindibili esigenze organizzative e istituzionali, per la sicurezza del lavoro e per la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, l'ente potrà, nei limiti di quanto previsto nel presente Regolamento e sulla base delle norme indicate, accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

5. Controlli

Premesso che non sono installati o configurati, sui sistemi informatici in uso agli utenti, apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori, l'Ordine si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.

I controlli vengono effettuati dal Consigliere all'uopo designato con l'ausilio dell'assistenza tecnica, anche dietro segnalazione proveniente dagli organi di polizia giudiziaria.

5.1 Principi

La prevenzione deve prevalere rispetto all'attività di controllo. Il COA si impegna pertanto a potenziare tale attività, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine.

I controlli effettuati dal COA rispettano i seguenti principi:
a. necessità: i dati trattati durante l'attività di controllo sono sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 5.2;

b. proporzionalità: i controlli sono sempre effettuati con modalità tali da garantire la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate al paragrafo 5.2;
c. imparzialità: i controlli sono effettuati su tutta la strumentazione informatica messa a disposizione dall'Ordine e conseguentemente possono coinvolgere tutti i collaboratori, a qualunque titolo utilizzino tale strumentazione, fatta eccezione per quella assegnata alle rappresentanze sindacali unitarie e agli organi istituzionali. In nessun caso sono effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie;
d. trasparenza: l'amministrazione mette in atto tutte le azioni necessarie a garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente regolamento. Sono pertanto informati dei possibili controlli tutti i soggetti di cui al precedente punto 2);
e. protezione dei dati personali: i controlli sono in ogni caso effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati sono conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. Oltre a quanto specificato sopra, i controlli sono effettuati rispettando la normativa vigente in materia di protezione dei dati personali.

5.2 Finalità

I controlli sono effettuati per le seguenti finalità:

a. evitare comportamenti impropri e/o potenzialmente dannosi per l'ente, che possano comportare anche l'irrogazione di sanzioni disciplinari;
b. evitare o comunque ridurre i rischi di un coinvolgimento civile e penale dell'Ordine, nel caso di illeciti nei confronti di terzi, commessi mediante l'utilizzo improprio dei beni messi a disposizione dall'amministrazione;
c. assicurare la continuità dei compiti istituzionali e tutelare l'immagine dell'Ordine e di coloro che vi prestano la propria attività.

5.3 Modalità di effettuazione dei controlli

Il controllo è effettuato su strumentazioni informatiche determinate o su account di posta elettronica a seguito di specifica segnalazione effettuata da un soggetto terzo oppure a seguito ad una verifica di sicurezza.
Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, il Presidente o altro soggetto dal medesimo incaricato deve dare informazione di tale controllo all'interessato, specificando che quest'ultimo può presentare richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990.
Le segnalazioni di un soggetto terzo sono ritenute più attendibili se non siano anonime e rivolte per iscritto al Presidente.

La verifica di sicurezza consiste in una attività di controllo da parte di uno dei soggetti sopra indicati i quali – anche con l'ausilio di personale tecnico specializzato - dopo aver rilevato elementi che possano configurare un utilizzo improprio delle strumentazioni informatiche, anche mediante ulteriori accertamenti, comunicheranno i dati strettamente necessari acquisiti attraverso tale controllo al COA, al C.d.A. di Fondazione Forense, al diverso datore di lavoro o responsabile della struttura di appartenenza o titolare dell'azione disciplinare del collaboratore interessato, che potranno effettuare

le ulteriori valutazioni e adottare le azioni conseguenti.
Gli ulteriori accertamenti sopraindicati possono ricomprendere controlli sull'account di posta elettronica, sui file archiviati e sui log dei siti di navigazione in Internet (in tale ultima ipotesi, solo nel caso in cui le relative informazioni siano indispensabili al fine di rilevare un utilizzo proprio o improprio dello strumento informatico.
Tutte le informazioni eventualmente raccolte saranno utilizzate a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679.

Qualora, anche a seguito delle ulteriori verifiche effettuate, siano riscontrati elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dall'Ordine, sarà associato il nominativo dell'utilizzatore alla postazione client, per poi procedere come di seguito disciplinato:
a. trasmissione all'organo di riferimento del soggetto coinvolto di un "verbale di controllo" affinché possa effettuare le valutazioni conseguenti, con particolare riferimento a una verifica relativa alla pertinenza o stretta attinenza dei dati di navigazione, indicati sul verbale stesso, con l'attività lavorativa;
b. contestuale comunicazione al soggetto coinvolto.

Nel caso in cui il soggetto coinvolto sia un dipendente dell'Ordine, la verifica di pertinenza con l'attività lavorativa, effettuata dal Presidente o dal soggetto da questi designato, deve comprendere la tempestiva audizione del soggetto controllato, affinché quest'ultimo possa fornire chiarimenti, motivazioni ed osservazioni in merito a quanto rilevato. All'audizione potranno essere presenti, su richiesta del COA o del soggetto coinvolto nel controllo, uno dei soggetti indicati al comma 1 o il tecnico da questi ultimi individuato.

A seguito delle verifiche sopra specificate, il Presidente (anche per il tramite del Consigliere designato) comunica per iscritto e senza ritardo, all'utilizzatore, l'esito del controllo e adotta nel contempo le opportune misure tecniche/organizzative per evitare il ripetersi del comportamento anomalo. Nel caso in cui dall'accertamento emergano responsabilità del dipendente per un uso gravemente improprio della strumentazione informatica, il COA avvia il conseguente procedimento disciplinare.