REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE AZIENDALI

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'A.S.P. Opere Sociali di N. S. di Misericordia di Savona (A.S.P. nel prosieguo) e gli utenti (dipendenti e collaboratori) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il presente regolamento è diretto a rendere note e precisare le regole di corretto utilizzo dei sistemi informatici.

Considerato inoltre che l'A.S.P., nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei collaboratori che ne necessitano per il tipo di funzioni svolte, telefoni e mezzi di comunicazione, vengono richiamate nel presente Regolamento le modalità ed ai doveri che ciascun collaboratore deve rispettare nell'utilizzo di tale strumentazione.

Le indicazioni che seguono integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

1. Campo di applicazione

1.1. Le presenti indicazioni devono essere osservate da tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori dell'A.S.P. a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

1.2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, co.co.co, ecc.) in possesso di specifiche credenziali di autenticazione (login/password). Tale figura potrà anche venir indicata quale "incaricato del trattamento".

2. Utilizzo del Personal Computer

2.1. Il Personal Computer affidato all'utente è uno strumento di lavoro e come tale da utilizzare nell'ambito dell'attività lavorativa e dei fini istituzionali. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2.2. Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete dell'A.S.P. solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 3 del presente regolamento.

2.3. Si informa che le persone incaricate alla gestione e alla manutenzione degli aspetti informatici dell'A.S.P ("addetti IT", nel prosieguo) sono autorizzate a compiere interventi sul sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché la verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.

2.4. Gli addetti IT hanno la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

2.5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dagli addetti IT né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa A.S.P. a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente. Eventuali programmi e banche dati regolarmente acquistati possono essere installati e ricevere manutenzione a cura dei tecnici della ditta fornitrice, dopo averne dato informazione alla Direzione e agli addetti IT.

2.6. Salvo preventiva espressa autorizzazione della Direzione, non è consentito all'utente di modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

2.7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 9 del presente regolamento relativo alle procedure di protezione antivirus.

2.8. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici. Analoga operazione va effettuata in caso di assenze prolungate dall'ufficio tenuto conto che un elaboratore 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[1].

3. Gestione ed assegnazione delle credenziali di autenticazione

3.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dagli addetti IT, su richiesta della Direzione.

3.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dagli addetti IT, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte della Direzione.

3.3. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

3.4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi.

3.5. Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con gli addetti IT.

3.6. Nel caso in cui si dovessero utilizzare le credenziali di un utente per accedere alle sue risorse, la Direzione può richiedere agli addetti IT l'azzeramento delle password, motivandone le cause e dando successivamente comunicazione all'interessato dell'avvenuto accesso.

4. Utilizzo della rete dell'A.S.P.

4.1. Per l'accesso alla rete dell'A.S.P. ciascun utente deve essere in possesso di specifiche credenziali di autenticazione.

4.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

4.3. Le cartelle utenti presenti nei server dell'A.S.P. sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non vi può essere dislocato, nemmeno per brevi periodi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte degli addetti IT. Si ricorda che i dischi e le altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte degli addetti IT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

4.4. Gli addetti IT possono in qualunque momento procedere alla rimozione di file o applicazioni che riterranno essere pericolosi per la sicurezza, sia sui PC che sulle unità di rete.

4.5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5. Utilizzo e conservazione dei supporti rimovibili

[1] Una modalità automatica che evita di lasciare incustodito il PC, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il savescreen a tempo con obbligo di reintrodurre la password per l'accesso.

5.1. Tutti i supporti rimovibili (supporti USB, hard-disk esterni, ecc.) contenenti dati di categorie particolari[2] devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto oppure, successivamente alla cancellazione, recuperato.

5.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati di categorie particolari, ciascun utente potrà contattare gli addetti IT e seguire le istruzioni da questo impartite.

5.3. In ogni caso, i supporti rimuovibili contenenti dati di categorie particolari devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

5.4. E' vietato l'utilizzo di supporti rimovibili personali, salvo casi in cui tale utilizzo sia necessario per lo svolgimento di attività lavorative, prestando la dovuta attenzione sulla provenienza di tali supporti e la necessaria diligenza nella conservazione degli stessi.

5.5. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

6. Utilizzo di PC portatili

6.1. L'utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

6.2. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

6.3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutte le cautele necessarie per evitare danni o sottrazioni.

7. Uso della posta elettronica

7.1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

7.2. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali non legati all'attività lavorativa;
- la partecipazione a piattaforme social, dibattiti, forum, aste elettroniche, mailing list, chat, ecc.

7.3. L'utilizzo della posta elettronica per la trasmissione di messaggi personali può essere consentita esclusivamente per brevi comunicazioni di tipo personale/familiare, in caso di necessità o quando tale forma di comunicazione consenta un risparmio di tempo rispetto all'uso di altri sistemi.

7.4. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

7.5. Al fine di garantire la funzionalità del servizio di posta elettronica, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) mette a disposizione di ciascun lavoratore una apposita funzionalità di sistema, di agevole utilizzo, che consente di inviare automaticamente

[2] I dati di categorie particolari sono, ai sensi dell'art.9 del GDPR, i seguenti: "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

messaggi di risposta contenenti le coordinate (elettroniche o telefoniche) di altro soggetto o altre utili modalità di contatto della struttura.

7.6. In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa o non voglia essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura degli addetti IT, su richiesta della Direzione o dell'interessato.

7.7. Gli addetti IT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potranno accedere alla casella di posta elettronica per le sole finalità indicate al punto 2.3. [3]

8. Navigazione in Internet

8.1. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa o comunque pertinenti l'attività lavorativa.

8.2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- Inviare o ricevere programmi ancorché gratuiti (freeware e/o shareware), nonché documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovranno venire a tal fine contattati gli addetti IT);
- Effettuare transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili; può ritenersi compatibile con il principio sopra indicato un occasionale utilizzo di internet per assolvere incombenze amministrative o burocratiche senza allontanarsi dal luogo di lavoro.
- Registrarsi a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- Partecipare a forum e chat non espressamente autorizzati della Direzione.

9. Protezione antivirus

9.1. Il sistema informatico dell'A.S.P. è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

9.2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto agli addetti IT.

9.3. Ogni dispositivo magnetico di provenienza esterna all'A.S.P. dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato agli addetti IT.

10. Utilizzo dei telefoni, fax e fotocopiatrici

10.1. Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione.

10.2. Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del

[3] L'accesso ai contenuti della corrispondenza nella casella di posta elettronica avviene esclusivamente in caso di assenza prolungata od impedimento dell'utente secondo quanto prescritto dal punto 10 del disciplinare tecnico legato al codice.

telefono: in particolare, è vietato l'utilizzo del telefono cellulare messo a disposizione per comunicazioni di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

10.3. È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte della Direzione.

11. Osservanza delle disposizioni in materia di Privacy

11.1. È obbligatorio attenersi alle disposizioni in materia di Privacy (GDPR) e di misure di sicurezza, come indicato nella lettera di autorizzazione al trattamento dei dati per conto del titolare.

12. Accesso ai dati trattati dall'utente

12.1. Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, tramite gli addetti IT, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

13. Sistemi di controlli graduali

13.1. L'A.S.P., utilizzando sistemi informativi anche per esigenze produttive o organizzative (ad es. per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si possono rivelare necessari per la sicurezza sul lavoro, potrà avvalersi legittimamente - nel rispetto dell'art. 4, comma 2 dello Statuto dei Lavoratori - di sistemi che potranno consentire indirettamente un controllo a distanza dei lavoratori e che potranno determinare un trattamento di dati personali riferiti o riferibili ai lavoratori. Qualora ciò avvenisse, nel rispetto di quanto previsto dal paragrafo 5 del Provvedimento generale del Garante "Linee guida del Garante per posta elettronica e internet", verrà data agli interessati opportuna informazione attraverso una comunicazione specifica della Direzione.

13.2. L'A.S.P non svolge e non svolgerà in futuro trattamenti di dati personali mediante sistemi hardware e software dedicati al controllo a distanza dei lavoratori, grazie ai quali potrebbe essere possibile ricostruire le loro attività e che sarebbero svolti tramite i seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire il servizio di posta elettronica;
- riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal dipendente;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso a internet o l'uso della posta elettronica messi a disposizione dei dipendenti.

13.3. I dati anonimi aggregati riferibili all'intera A.S.P. o a sue aree, qualora venissero trattati, saranno a disposizione della Direzione per le valutazioni di competenza e potranno riguardare:

- per ciascun sito/dominio visitato: il numero di utenti che lo visitano, il numero delle pagine richieste e la quantità di dati scaricati;
- per ciascun utente, presentato in forma anonima: il numero di siti visitati e la quantità totale di dati scaricati.

13.4. Qualora venissero utilizzati "log di tracciatura", i dati personali eventualmente presenti in tali log saranno trattati in forma non anonima in via eccezionale ed esclusivamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati), se persiste nel mese successivo alla rilevazione anonima, l'utilizzo anomalo, nonostante la diffida a cessare tale comportamento.

13.5. Nei casi in cui i soggetti preposti alle verifiche accertino utilizzi anomali degli strumenti, sono tenuti a darne comunicazione riservata alla Direzione.

13.6. Qualora venissero utilizzati log di tracciatura, i dati contenuti nei log stessi saranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a sei mesi, e saranno periodicamente e automaticamente cancellati dal sistema.

13.7. Relativamente ai trattamenti di cui ai punti del presente paragrafo, nel caso in cui vengano effettuati, sarà data agli interessati opportuna informazione attraverso una comunicazione specifica della Direzione.

14. **Sanzioni**

14.1. È fatto obbligo a tutti gli utenti di osservare le disposizioni contenute nel presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente ordinamento, nonché con tutte le azioni civili e penali consentite.

Il presente regolamento viene pubblicato sulla bacheca aziendale e consegnato a ciascun utente.

Savona, 12 Aprile 2021

Il Direttore