DISCIPLINARE INTERNO SULL'USO DI INTERNET, POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI

Disciplinare approvato con decreto del Presidente n 94 dd. _25.10.2023

Sommario

INTRODUZIONE

La Comunità della Valle di Sole mette a disposizione del proprio personale e di eventuali collaboratori esterni, stagisti e tirocinanti i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale, quali personal computer e relativi accessori, scanner ecc.
- apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti di rete fileserver ecc.
- programmi di produttività individuale e procedure gestionali.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.

Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi.

In particolare si evidenzia come l'utilizzo delle risorse informatiche per scopi non inerenti all'attività lavorativa possa contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle infrastrutture della Comunità.

Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare:

- Regolamento UE 2016/679 e successiva regolamentazione con D. Lgs. 101/2018;
- provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali, in particolare il provvedimento 1 marzo 2017 "Linee guida del Garante per posta elettronica e internet";
- circolari dell'Agenzia per l'Italia Digitale (AGID), in particolare la circ. 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)".

La Comunità Della Valle di Sole non effettua registrazioni per il controllo dell'attività lavorativa dei dipendenti, ma solo registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi. I dati registrati automaticamente a tale scopo non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

CAMPO DI APPLICAZIONE

Le regole descritte nel presente documento devono essere rispettate da tutto il personale della Comunità della Valle di Sole (inclusi i consulenti esterni, stagisti e tirocinanti), indipendentemente dal tipo di incarico svolto e dalla sede dell'attività.

La gestione delle risorse strumentali, ivi incluse quelle informatiche, compete ai Responsabili di Settore per la parte delegata, i quali si assumono le responsabilità legate al corretto utilizzo ed all'osservanza delle norme.

È responsabilità di tutti i soggetti che utilizzano i personal computer ed altri dispositivi elettronici, la posta elettronica e internet messi a disposizione dalla Comunità della Valle di Sole applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

NORMATIVA DI RIFERIMENTO

Il presente Disciplinare Interno è redatto in conformità alla normativa vigente, di seguito riportata per riferimento:

- Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n. 633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione;

- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art. 171 della Legge n. 633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n. 248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie;

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori);

- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge";

- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza;

- Regolamento 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);

- Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l’adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull’utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di: evitare possibili distruzioni, perdite, alterazioni di dati; garantire che l’accesso ai dati sia effettuato dalle sole persone incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite;

- Circolare Agenzia per l’Italia Digitale 18 aprile 2017, n. 2/2017 “Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)”;

- Le misure di sicurezza sono applicate garantendo il rispetto di quanto disposto dalle “Linee guida del Garante per posta elettronica e internet” emesse dall’Autorità Garante per la protezione dei dati personali il 1 marzo 2007.

UTILIZZO DELLE POSTAZIONI DI LAVORO

Principi generali

In funzione del proprio ruolo delle esigenze organizzative e lavorative, il personale in servizio presso la Comunità della Valle di Sole è dotato di personal computer e/o altri dispositivi per lo svolgimento di attività connesse agli incarichi lavorativi, nel rispetto delle regole di seguito descritte.

Il personal computer e gli eventuali altri dispositivi sono assegnati nominalmente al dipendente e sono a tutti gli effetti uno strumento di lavoro. Ognuno è responsabile dell’utilizzo delle dotazioni informatiche ricevute in assegnazione dalla Comunità.

Le pubbliche amministrazioni sono tenute ad assicurare il corretto impiego degli strumenti ICT e della telefonia da parte dei propri operatori, definendone le modalità di utilizzo nell’organizzazione dell’attività lavorativa. Questo avviene nell’ottica di garantire la sicurezza, la disponibilità e l’integrità dei sistemi e di prevenire sprechi. Esiste quindi in capo agli operatori l’obbligo, sancito da norme di legge e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, e questo anche nell’utilizzo delle risorse aziendali. In particolare l’art. 3 comma 4 del Codice di comportamento dei dipendenti della Comunità della Valle di Sole, adottato con delibera di Giunta n. 4 di data 29.01.2015 modificato con deliberazione 33 del 20.03.2019, prevede che “*Il dipendente usa e custodisce con cura i beni di cui dispone per ragioni di ufficio e non utilizza a fini privati le informazioni di cui dispone per ragioni di ufficio*”. Tale prescrizione riguarda quindi anche l’uso delle risorse informatiche, nell’utilizzo delle quali il dipendente deve agire in modo da non pregiudicare e ostacolare le attività dell’Ente o perseguire interessi privati in contrasto con quelli pubblici-.

Viene quindi posto l’obbligo, in carico ai Responsabili di settore ed ai preposti, di vigilanza sugli operatori delle proprie strutture al fine di verificare l’effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro. Ogni abuso in tal senso dovrà essere prontamente rilevato ed eventualmente sanzionato.

Regole di utilizzo

Le postazioni di lavoro, normalmente, sono connesse alla rete interna della Comunità con lo scopo di usufruire dei servizi dell'Ente, accedere alle applicazioni software gestite centralmente dall'Ufficio Informatica, condividere informazioni, fruire i contenuti dell'Intranet.

Per accedere ai servizi dalla propria postazione di lavoro l'utente deve utilizzare delle credenziali, in particolare un codice identificativo (nome utente del tipo<cognome><iniziale del nome>) ed una parola chiave segreta (password). In caso di necessità operativa è sempre possibile, da parte di ciascun utente, accedere alla rete tramite un'altra postazione utilizzando le proprie credenziali.

Per una corretta gestione delle postazioni di lavoro è necessario osservare alcune regole:

- le informazioni archiviate nella postazione devono essere esclusivamente quelle inerenti la propria attività lavorativa;
- la modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche messe a disposizione è di esclusiva competenza dell'Amministratore di Sistema;
- la modifica delle configurazioni software, impostate sulla propria o altrui postazione di lavoro, è consentita esclusivamente all'Amministratore di Sistema: l'utente può eventualmente procedere ad eventuali modifiche solo dopo aver avuto esplicita autorizzazione a farlo;
- non è consentita l'installazione di programmi applicativi diversi da quelli predisposti e/o autorizzati dall'Amministratore di Sistema inclusi, tra gli altri, browser per la navigazione internet e software di *office automation*. Le richieste di installazione e aggiornamento di ulteriori applicativi rispetto a quelli autorizzati devono essere preventivamente validate dall'Amministratore di Sistema in ordine alle necessarie verifiche tecniche. Qualora venissero riscontrati programmi non autorizzati sulle postazioni di lavoro, anche se legali, questi verranno disinstallati dal personale tecnico addetto alla manutenzione delle postazioni di lavoro;
- non è consentito utilizzare risorse informatiche private (tablet, smartphone, periferiche etc.), salvo preventiva ed esplicita autorizzazione dall'Amministratore di Sistema; in caso di autorizzazione, l'utente è tenuto a rispettare il contenuto del presente disciplinare;
- la riproduzione o la duplicazione di programmi può essere effettuata solo nel pieno rispetto della vigente normativa in materia di protezione della proprietà intellettuale;
- si sconsiglia l'uso di pendrive, hard disk esterni, DVD o analoghi supporti di memorizzazione di incerta provenienza, che potrebbero causare danni alla postazione di lavoro; l'uso di memorie USB, data l'estrema facilità con cui possono prestarsi alla diffusione di virus e malware, è da evitare;
- è proibito duplicare documenti contenenti dati sensibili su supporti removibili o su sistemi di rete non gestiti dal personale della Comunità (ad es. su cloud esterno);
- è vietata l'installazione non autorizzata di propri dispositivi di connessione come Access Point, router, print server, modem, ecc… alla rete della Comunità;

- in caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, informare tempestivamente l'Amministratore di Sistema comunicando quali dati erano contenuti all'interno;

- in caso di allontanamento anche temporaneo dalla propria postazione di lavoro è opportuno bloccare il personal computer. Si ricorda che, in caso di allontanamento temporaneo e trascorsi 7 minuti di inattività, il sistema in modo automatico attiva un blocco della sessione utente con salva schermo sbloccabile solo con l'inserimento della password utente;

- al termine del lavoro devono essere correttamente chiusi tutti gli applicativi e la sessione di lavoro, e devono essere spenti computer, video ed accessori anche al fine di evitare sprechi energetici ed inutile usura del personal computer. Viene fatta eccezione per gli utenti che svolgono prestazione lavorativa parte in presenza e parte in modalità smart-working, per i quali, al termine dell'attività lavorativa, è obbligatorio chiudere tutte le applicazioni attive, disconnettere il proprio utente da qualsiasi sessione web in-cloud, compreso l'utente di posta elettronica, e disconnettere l'utente senza spegnere il terminale. È sempre consigliato spegnere il monitor al termine della sessione di lavoro al terminale;

- posto che vi è la necessità di utilizzare gli spazi di archiviazione e memoria in maniera ottimale, gli operatori devono effettuare con cadenza periodica (almeno ogni sei mesi, ossia entro il 30/06 ed entro il 31/12 di ciascun anno solare) l'eliminazione dei *files* inutili, duplicati o per i quali va rispettata una scadenza nella conservazione dei dati presenti nel PC in uso e nelle cartelle di rete di propria competenza;

- va evitata l'archiviazione ridondante, sia sul PC in uso, sia sulle cartelle server di sistema, attraverso il salvataggio di *files* già presenti e reperibili in applicazioni e banche dati specifiche (es. PiTre, …), o salvando anche in formato .pdf *files* già salvati in formato editabile;

- nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali (impostando ad esempio una password a protezione di queste banche dati).

L'utente è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza segnalando tempestivamente all'Amministratore di Sistema ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro.

Le suddette norme comportamentali devono essere osservate anche nei casi di utilizzo di risorse informatiche non fornite direttamente dall'Amministratore di Sistema, ma acquisite a vario titolo nel corso del tempo.

Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, la Comunità utilizza alcuni software che permettono all'Amministratore di Sistema di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente. L'attivazione di tale funzionalità può essere richiesta solamente da parte dell'Amministratore di Sistema e solo quando strettamente necessario per poter svolgere l'attività di assistenza tecnica informatica, Deve essere sottoposta ad un preventivo e contestuale consenso da parte del lavoratore e avviene sotto la sua totale supervisione.

Modalità di utilizzo di postazioni “mobili”

L’Ente consegna a specifici dipendenti personal computer portatili. Le regole di utilizzo di queste apparecchiature sono le stesse dei personal computer collegati alla rete locale anche se i servizi disponibili e la loro modalità di erogazione potrebbe differenziarsi dalle postazioni 'fisse'.

Il loro utilizzo richiede inoltre maggiori precauzioni rispetto alle postazioni fisse in ordine ai seguenti elementi:

- attenzione rispetto al furto o allo smarrimento;
- attenzione rispetto a virus o codici maligni tramite reti wireless (senza fili).

I portatili che rimangono sconnessi dalla rete intranet aziendale, ricevono comunque gli aggiornamenti delle definizioni antivirus ogni qualvolta si connettono alla rete Internet, garantendo così una protezione continua del dispositivo anche se lo stesso rimane sconnesso a lungo dalla rete intranet aziendale. Eventuali aggiornamenti del software antivirus sono possibili solo quando il dispositivo risulta collegato alla rete wifi indoor aziendale o mediante accesso da remoto via VPN (Virtual Private Network) alla rete aziendale.

Per quanto riguarda le smart card, business key e altri dispositivi per il riconoscimento che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell’Ente, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo.

CREDENZIALI E PASSWORD

Principi generali

Le credenziali (nome utente e password) per l’accesso ai servizi informatici della Comunità della Valle di Sole vengono rilasciate dall’Amministratore di Sistema previa richiesta da parte del Responsabile di Settore dell’utente interessato, con contestuale fornitura dei dati identificativi necessari alla creazione (nome, cognome, codice fiscale, settore di appartenenza, visibilità sulle connessioni di rete del file server, visibilità sulle caselle di posta elettronica ordinaria di servizio, accesso a servizi web, data di inizio servizio).

La richiesta di rilascio deve avvenire da parte del Responsabile di Settore mediante mail all’Amministratore di Sistema, con un preavviso di almeno 3 giorni lavorativi.

L’Amministratore di Sistema provvede a rigenerare password di primo accesso dimenticate dall’utente con obbligo di modifica al primo accesso e a disattivare le utenze per gli utenti che cessano la propria attività lavorativa.

L’esecuzione di operazioni di assistenza sulle postazioni di lavoro che richiedono l’utilizzo di un’utenza con diritti amministrativi, sono eseguite dall’Amministratore di Sistema sotto la supervisione dell’utente assegnatario della postazione, salvo nei casi in cui vi sia l’urgenza di intervenire in assenza dell’utente. L’Amministratore di Sistema esegue anche ogni attività di assistenza per conto di fornitori terzi che richieda l’esecuzione di operazioni con diritti amministrativi. Nessuna utenza con diritti amministrativi viene rilasciata né all’utente aziendale, né a fornitori terzi.

L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi della Comunità, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, abuso della propria posta elettronica etc.); inoltre questo comportamento può esporlo a responsabilità civile e penale per eventuali utilizzi illeciti.

Regole di utilizzo

Per una corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole:

- modificare alla prima connessione la password che l'amministratore di sistema attribuisce e comunica;

- le password aziendali devono contenere:
  a) almeno una lettera maiuscola
  b) almeno una lettera minuscola
  c) almeno una cifra
  d) almeno un carattere di punteggiatura in sostituzione di uno dei caratteri di cui ai precedenti punti a,b,c
  e) lunghezza minima 10 caratteri
  f) non devono contenere nessun riferimento con il nome e cognome dell'utente
  g) devono essere diverse dalle ultime 3 password usate

- modificare la password almeno ogni 90 giorni e, nel caso in cui si ritenga che la propria password sia stata compromessa, modificarla immediatamente;
- mantenere la password riservata, non lasciarla incustodita o in vista sulla propria postazione di lavoro, non divulgarla a terzi: l'utente è responsabile penalmente e civilmente di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali;
- non trascriverla su supporti facilmente accessibili a terzi (ad es. foglietti, post-it, ecc.);
- non permettere ad altri utenti o colleghi di operare con le proprie credenziali;
- comunicare tempestivamente all'Amministratore di Sistema trasferimenti e cessazioni, in modo da consentire la disabilitazione dell'accesso ai servizi non strettamente necessari.

USO DELLA POSTA ELETTRONICA

Principi generali

La Comunità della Valle di Sole fornisce un servizio di posta elettronica, mettendo a disposizione indirizzi con estensione @comunitavalledisole.tn.it; gli indirizzi possono essere individuali o per servizio, questi ultimi vengono richiesti dal responsabile dello stesso e condivisi tra più dipendenti. Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Il database di posta è di esclusiva proprietà dell'Ente, l'Amministratore di Sistema per motivi tecnici e di sicurezza, in particolare per prevenire o correggere malfunzionamenti, può accedere al suo contenuto nel rispetto della normativa vigente.

Regole di utilizzo

Per l'uso del servizio di posta elettronica si richiede di osservare le seguenti norme comportamentali:

- l'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle mansioni assegnate; l'utente del servizio è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa;
- collegarsi al server di posta (sia dall'interno che dall'esterno della rete della Comunità) all'indirizzo https://mail.google.com; l'Amministratore di Sistema fornisce assistenza all'uso ed alla configurazione esclusivamente per i programmi *client* autorizzati;
- al fine di sfruttare razionalmente lo spazio disponibile per la memorizzazione, ogni utente è soggetto a limiti di utilizzazione; il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi fino a quando non viene liberato spazio sufficiente. Ogni singolo utente deve verificare la percentuale di occupazione del suo spazio di archiviazione;
- il titolare di indirizzo di posta elettronica ha il dovere di controllare periodicamente la propria casella elettronica, verificare l'arrivo di nuovi messaggi, cancellare i messaggi obsoleti o inutili, verificare lo spazio occupato, prestare attenzione ai messaggi di quota raggiunta, ripulire la casella di posta prima del raggiungimento della quota massima consentita;
- limitare la dimensione dei messaggi inviati, soprattutto nel caso di destinatari multipli; un allegato di grandi dimensioni potrebbe impedire il corretto smistamento del messaggio o richiedere un uso eccessivo delle risorse;
- qualora sia necessario ricevere o spedire documenti di dimensioni maggiori del normale (sopra i 25 GB), è necessario utilizzare Google Drive o altri servizi di condivisione di file (Wetransfer);
- è richiesto, nei messaggi in uscita, riportare in calce la firma del soggetto mittente contenente, al minimo: nome, cognome ed Ufficio/Settore di appartenenza;
- è necessario porre particolare attenzione ad aprire allegati alle mail di tipo criptato, contenenti script non verificati. In linea generale è vietato aprire allegati se l'email sembra sospetta, anche per un mittente conosciuto di cui però non è possibile accertarne l'autenticità. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di *phishing* o frodi informatiche. In qualunque situazione di incertezza contattare l'Amministratore di Sistema per una valutazione dei singoli casi. Si consiglia inoltre di:
    - prestare la massima attenzione all'inserimento delle vostre credenziali e dati personali all'interno di portali a cui si accede seguendo link ricevuti tramite messaggio;
    - non aprire file collegati o presenti in mail per le quali non abbiate la sicurezza del mittente e non ci sia coerenza con le attività lavorative;
- è illecito scambiare messaggi sotto falsa identità, ovvero impersonando un altro mittente;
- dato il carattere istituzionale delle caselle di posta della Comunità della Valle di Sole è fatto divieto inoltrare all'esterno messaggi non inerenti le proprie competenze nell'Ente ed utilizzare l'indirizzo di posta per motivi non legati all'attività lavorativa ed istituzionale. In particolare, è fatto divieto utilizzare l'account di posta elettronica di lavoro per registrarsi su portali ad uso personale;

- poiché la posta elettronica diretta all'esterno della rete informatica comunitaria può essere intercettata da estranei, è da evitare di mantenere a lungo nella propria casella di posta informazioni/documenti riservati dopo averli inviate ai destinatari, per evitare che qualcuno se ne appropri nel caso di accesso non autorizzato al contenuto della casella di posta;
- non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo;
- assicurarsi che nei messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre applicazioni. In particolare va usata la massima cautela nell'invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata;
- è necessario prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari;
- si raccomanda di prestare la massima attenzione nella selezione dei destinatari, qualora l'utente abbia selezionato l'opzione di completamento automatico dell'indirizzo, al fine di evitare l'invio di messaggi elettronici a destinatari diversi da quelli effettivamente desiderati. A tal proposito, si ricorda che una email contenente dati personali inviata per errore ad uno o più destinatari costituisce una **violazione della privacy (c.d. caso di DATA BREACH), da segnalare tempestivamente all'Ufficio Segreteria secondo la procedura adottata dall'Ente;**
- è possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata un'importanza relativa poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio;
- in caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, l'indirizzo di un collega o del Settore/Ufficio di riferimento che può essere contattato in sua assenza;
- alla cessazione dell'attività lavorativa presso la Comunità, la casella di posta del dipendente sarà disattivata e successivamente eliminata in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure atte a informare e a fornire a terzi, in modalità automatica, gli indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. La predisposizione di tali strumenti automatici è a carico del dipendente che cessa il rapporto di lavoro.

USO DELLA RETE LOCALE, INTERNET E RISORSE CONDIVISE

Principi generali

Di norma ogni postazione di lavoro è connessa alla rete locale della Comunità ed agli utenti sono fornite le credenziali per l'accesso alla intranet, ad internet ed alle risorse di rete condivise funzionali all'attività lavorativa. Tali accessi devono avvenire esclusivamente per finalità istituzionali, strettamente connesse agli incarichi lavorativi svolti e sempre nel rispetto delle regole elencate in questo documento.

Regole di utilizzo

Per l'uso dei servizi connessi ad internet, alla rete locale ed alle risorse di rete condivise, valgono le seguenti norme comportamentali:

- non è consentito navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate;
- non trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer;
- non scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo e comunque sempre e solo per attività connesse alle esigenze lavorative;
- non è consentito l'uso di programmi *peer to peer* per lo scambio di file in ambito privato (ad es. BitTorrent, eMule, iMesh, Limeware);
- non partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network. Nel caso di riunioni organizzate dall'Ente (es. tramite piattaforme Meet, Lifesize, ecc...) è consigliabile impostare una password di accesso;
- non pubblicare testi, immagini o video a contenuto blasfemo, osceno o diffamatorio;
- è vietata ogni forma di registrazione a nome della Comunità o fornendo i dati relativi ad e-mail della Comunità a siti i cui contenuti non siano legati all'attività lavorativa;
- cercare di limitare, ogni volta che sia possibile, le stampe, in modo da risparmiare preziose risorse;
- ad ogni utente e ad ogni ufficio viene assegnato uno spazio sui file server centrali; le cartelle presenti nel server sono aree di salvataggio e/o condivisione di informazioni strettamente professionali: non possono in alcun modo essere utilizzate per scopi diversi;
- i documenti e tutto il materiale prodotti in ragione del proprio ruolo all'interno dell'Ente devono essere regolarmente salvati nelle cartelle appositamente create sul server aziendale, ciò anche al fine di garantire la continuità operativa degli uffici in caso di assenza del dipendente e/o di emergenza (i dati non vanno pertanto salvati sulla postazione individuale o sul *desktop*);
- il materiale non pertinente all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, su personal computer o sulle cartelle di rete condivise. L'Amministratore di Sistema può procedere in ogni momento alla rimozione di materiale ritenuto non pertinente o potenzialmente pericoloso senza preavviso;
- sulle unità di rete condivise vengono svolte regolari attività di controllo, amministrazione e back up da parte dell'Amministratore di Sistema, in caso di perdita dei dati è possibile rivolgersi all'Amministratore di Sistema per recuperare i dati mancanti;
- lo spazio disco messo a disposizione ha dei costi notevoli sia in termini economici che di tempo dedicato alla manutenzione, pertanto ogni utente periodicamente provvede alla cancellazione dei file obsoleti o inutili. Al superamento del limite individuale impostato per la quantità di informazioni, per validi e giustificati motivi, è possibile per il Responsabile di Settore richiedere all'Amministratore di Sistema un ampliamento dello spazio a disposizione;

- in generale è vietato ai dipendenti l'utilizzo di internet per svolgere qualsiasi attività che non rientri tra i compiti istituzionali (es: accesso alla propria posta personale, attività di carattere personale nei confronti di pubbliche amministrazioni, istituti bancari, vendita on-line, ecc.);

- ogni dipendente è tenuto a comunicare per iscritto (es. tramite email) al proprio Responsabile di Settore ed all'Amministratore di Sistema gli accreditamenti/registrazioni effettuati per motivi di lavoro, indicando il sito/portale e l'eventuale servizio abilitato (anche legati alla casella di posta elettronica del dipendente), ciò anche al fine di garantirne la disattivazione in caso di cessazione dal rapporto di lavoro.

Utilizzo dei telefoni, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà della Comunità Della Valle di Sole e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

- Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.
- Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.
- Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Ufficio CED.
- È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Settore.
- Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
    a) stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
    b) prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
    c) prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile;
    d) le stampanti locali dell'Ente devono essere spente in caso di inutilizzo prolungato.

Ai fini della tutela per la privacy, si raccomanda quanto segue:

- nel caso in cui si rendesse necessaria la stampa di informazioni riservate, l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate. Si dovrà prestare attenzione a non dimenticare l'originale del documento all'interno della macchina fotocopiatrice e/o dello scanner;
- per chi utilizza lo scanner centrale condiviso (fotocopiatore di piano), una volta effettuata la scansione, questa va subito **eliminata** dalla cartella del server accessibile a tutti, questo in particolar modo quando il documento contenga anche dati particolari (ex sensibili) e/o giudiziari.

L'Amministratore di Sistema è autorizzato alla cancellazione del contenuto della cartella SCANSIONI con periodicità settimanale senza alcun preavviso per l'utente.

Precauzioni generali da adottare con riferimento particolare al trattamento di dati personali contenuti in archivi e documenti cartacei

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Provinciale e vanno scartati nei tempi previsti dal Piano di conservazione adottato dalla Comunità con deliberazione del Comitato Esecutivo n. 48 dd. 26.11.2015.

I documenti contenenti dati particolari (ex sensibili e/o giudiziari) devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione.

L'archiviazione dei documenti cartacei contenenti dati particolari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave.

I documenti contenenti dati particolari vanno riposti negli appositi contenitori o armadi al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, i documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Settori.

La fase di cessazione prevede le seguenti modalità operative:

- le credenziali fornite all'utente verranno disabilitate: è cura del Responsabile di Settore interessato comunicare nominativo e data della cessazione dell'utente all'Amministratore di Sistema;
- allo stesso modo il Responsabile di Settore provvederà a disattivare l'accesso del dipendente che cessa la propria attività a favore della Comunità da eventuali altre banche dati alle quali ha avuto accesso unicamente in ragione del proprio servizio presso la Comunità;
- la casella di posta elettronica individuale verrà disattivata entro 7 giorni lavorativi e successivamente cancellata (entro 30 gg dalla data di cessazione): le attività necessarie per il passaggio delle consegne e la copia del materiale di interesse dell'Ufficio dovranno essere effettuati dall'interessato prima della cessazione dell'incarico, in modo tale da consentire la continuità del servizio erogato;
- le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore della Comunità della Valle di Sole restano nella piena ed esclusiva disponibilità della Comunità;

- l'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse della Comunità presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro a meno di esplicita autorizzazione scritta preventiva da parte del Responsabile della struttura di appartenenza;

- le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per la Comunità verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per l'Ente.

INTERVENTI DI ASSISTENZA E MANUTENZIONE

Principi generali

L'Amministratore di Sistema ha tra i suoi compiti quello di garantire il funzionamento generale della infrastruttura (sicurezza informatica, backup, rete, server, progettazione informatica ecc.) e dedica le proprie risorse in via prioritaria allo svolgimento di tali attività; le richieste di assistenza ai singoli vengono gestite con le modalità indicate di seguito.

Regole di utilizzo

Per le richieste di assistenza, valgono le seguenti norme comportamentali:

- le richieste vanno inoltrate inviando una mail alla casella segreteria@comunitavalledisole.tn.it o contattando telefonicamente l'Amministratore di Sistema, indicando chiaramente il tipo di inconveniente riscontrato ed ogni tipo di informazione utile a diagnosticare il problema, evitando indicazioni generiche come "non va", "non funziona", etc. Un messaggio di posta elettronica confermerà la presa in carico da parte del tecnico;

- le richieste vengono evase in ordine di ricezione, dando priorità agli interventi che coinvolgono più utenti o che mettono a rischio la continuità dei servizi erogati ai cittadini;

- lo svolgimento di attività che richiedono impegni finanziari per essere svolte, è soggetto a valutazioni di convenienza economica da parte dell'Amministratore di Sistema ed alla verifica della copertura finanziaria necessaria.

PROCEDURE DI ACQUISTO E SOSTITUZIONE

Il materiale informatico (hardware e software) è soggetto a guasti e ad obsolescenza e le risorse a disposizione di ogni ufficio possono risultare inadeguate per soddisfare le nuove esigenze che dovessero manifestarsi nel tempo.

L'acquisto e la sostituzione di prodotti informatici (hardware e software) prevede le seguenti modalità operative:

- ogni anno, entro il mese di ottobre/novembre, i Responsabili di Settore comunicano al Responsabile dell'Ufficio Informatica (attualmente il Segretario generale) le proprie necessità per l'anno successivo, al fine di permettere la redazione delle previsioni di bilancio per l'anno di competenza;

- in caso di richieste urgenti, ad esempio dovute a guasti o altri imprevisti, ogni utente si rapporta al proprio responsabile che – valutata l'effettiva necessità - provvede a compilare ed inoltrare richiesta via email all'Amministratore di Sistema;

- l'Amministratore di Sistema, valutata sul piano tecnico la congruità delle richieste pervenute e verificata l'adeguata copertura finanziaria, le inoltra al Responsabile dell'Ufficio Informatica (attualmente il Segretario generale) per l'effettiva procedura di acquisto;

- gli acquisti e le modifiche alle procedure informatiche (gestionali etc.) devono essere inderogabilmente sottoposte all'Amministratore di Sistema che provvederà all'analisi dei requisiti, alla valutazione del merito, della congruità tecnica e della compatibilità con gli attuali sistemi, al contatto con i fornitori ed al successivo supporto agli utenti.

SVILUPPO

Il Settore Segreteria, Istruzione e Personale provvede allo sviluppo dell'infrastruttura informatica dell'Ente e ne cura la successiva manutenzione.

La gestione di progetti congiunti con altri Settori o di programmi da condividersi fra più Settori è strutturata in modo tale per cui le attività aventi ricadute, anche indirette, sull'Ufficio Informatica della Comunità debbano prevedere il coinvolgimento dell'Amministratore di Sistema a partire dalla fase di progetto fino alla conclusione dei lavori, in modo da ottimizzare l'integrazione con l'infrastruttura esistente sia hardware che software con particolare riferimento alle attività legate a reti, cablaggi, procedure informatiche da ospitare in cloud o da alimentare con dati di pertinenza dell'Ente, evitando costose duplicazioni e pericolose incompatibilità.

CONTROLLI

- La Comunità della Valle di Sole, utilizzando sistemi informativi per esigenze produttive o organizzative (ad esempio per rilevare anomalie o per manutenzione), può avvalersi, nel rispetto dell'art. 4 comma 2 dello Statuto dei Lavoratori, di sistemi che permettano un controllo indiretto a distanza (controllo preterintenzionale) e determinano un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007;

- La Comunità non effettua, in alcun caso, trattamenti di dati personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti con i seguenti mezzi:

    - lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto tecnicamente necessario per fornire il servizio di posta stesso;
    - memorizzazione ed eventuale riproduzione delle pagine web visitate dal dipendente;
    - lettura e registrazione dei caratteri inseriti dai lavoratori mediante tastiera;
    - analisi occulta di computer affidati in uso;

- Le attività di controllo, legittimamente svolte dalla Comunità della Valle di Sole ai sensi del presente

disciplinare, si attengono in ogni caso ai seguenti principi fondamentali:

1. **Necessità, pertinenza e non eccedenza**: I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. La Comunità raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come "di rischio".
2. **Finalità e correttezza**: I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dalla Comunità riguardano o possono riguardare, caso per caso:
   - sicurezza sul lavoro
   - sicurezza dei sistemi e relativa risoluzione di problemi tecnici
   - esigenze di organizzazione
   - esigenze di produzione
   - rispetto di obblighi legali
   - tutela della Comunità

- Le attività che comportano l'uso del servizio di accesso ad internet sono monitorate attraverso l'uso di apparati firewall che in forma anonima memorizzano in file di log tutti gli accessi ad internet;
- I dati personali contenuti nei log possono essere trattati in forma non anonima solo in via eccezionale ed esclusivamente nelle ipotesi in cui si rilevino evidenze di un utilizzo improprio o illegale, ovvero sia necessario corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza – comunque non superiore a sei mesi – e sono cancellati periodicamente ed automaticamente dal sistema;
- I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

SANZIONI

L'inosservanza delle norme comportamentali descritte nel presente documento può comportare l'applicazione di sanzioni disciplinari ovvero di altre misure di tutela dell'Ente che si rendessero necessarie, incluso il risarcimento di eventuali danni arrecati alle apparecchiature, al software ed alle configurazioni in uso.

INFORMATIVA

Il presente Disciplinare costituisce preventiva e completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e successiva regolamentazione con D. Lgs. 101/2018 circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.

La Comunità della Valle di Sole assicura al presente Disciplinare ed ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti, mediante:

- pubblicazione nella intranet aziendale;
- comunicazione del testo a tutti i dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture della Comunità;
- pubblicazione del testo agli albi delle rappresentanze sindacali;
- consegna di copia del testo a tutti i futuri dipendenti e a coloro che a vario titolo presteranno servizio o attività per conto e nelle strutture della Comunità;
- pubblicazione del testo sul sito internet della Comunità.

CLAUSOLA DI REVISIONE

Il presente Disciplinare è aggiornato periodicamente in considerazione di:

− introduzione di nuovi strumenti elettronici, rilevanti per le finalità del Disciplinare;

− modifiche e/o innovazioni di carattere normativo o giurisprudenziale;

− modifiche e/o innovazioni di carattere tecnico-informatico;

− esperienze maturate, nel periodo di riferimento, in applicazione del disciplinare;

− nuove esigenze di sicurezza, produzione, organizzazione che giustifichino una revisione del Disciplinare.