COMUNE di
COCCAGLIO

DISPOSIZIONI PER L'UTILIZZO DISPOSITIVI INFORMATICI

Approvato con Deliberazione di Giunta Comunale n. 100 del 29/11/2024

Viale Matteotti n. 10, 25030 COCCAGLIO (BS) - C.F. 00821390176 – P.IVA 00580060986
protocollo@pec.comune.coccaglio.bs.it - www.comune.coccaglio.bs.it

Sommario

Art. 1 – Scopo e campo di applicazione

Le presenti disposizioni hanno lo scopo di fornire a dipendenti, collaboratori e amministratori del **Comune di Coccaglio** le modalità d'utilizzo degli strumenti informatici (anche con riferimento all'installazione ed utilizzo di programmi ed applicazioni software) e le istruzioni da seguire durante lo svolgimento delle attività lavorative che comportano un trattamento di dati personali, al fine di evitare che, anche inconsapevolmente, possano minacciare o compromettere la sicurezza del sistema informatico dell'Ente o la protezione dei dati ivi contenuti o arrecare un qualunque danno all'Ente (economico o di immagine).

Il diffondersi delle nuove tecnologie consente infatti al lavoratore, nell'adempimento delle mansioni assegnate, l'accesso a strumenti e servizi sempre più innovativi e performanti, ma, di riflesso, richiede l'adozione di precise etiche comportamentali, il rispetto delle norme in vigore e in generale dei principi di correttezza, diligenza e buona fede e di una condotta conforme ai civici doveri. Le prescrizioni di seguito indicate vogliono quindi porre l'attenzione sugli aspetti summenzionati.

Art. 2 – Responsabilità del documento

Il documento è soggetto ad una revisione periodica da parte dei responsabili della redazione.
Eventuali modifiche o integrazioni al documento possono essere suggerite da tutto il personale dipendente mediante comunicazione mail all'indirizzo segreteria@comune.coccaglio.bs.it.

Art. 3 – Responsabilità generali di tutti i lavoratori

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Amministrazione.

Il computer o altro apparato in dotazione al dipendente è configurato dall'Amministrazione in modo da consentirne l'utilizzo esclusivamente per finalità lavorative e per la salvaguardia della sicurezza e dell'integrità dei dati e dell'infrastruttura tecnologica.

Il/La dipendente è responsabile della sicurezza, custodia e conservazione in buono stato, salvo l'ordinaria usura derivante dall'utilizzo, delle dotazioni informatiche.

Il/La dipendente è tenuto/a a:

- utilizzare la dotazione esclusivamente per le attività inerenti al rapporto di lavoro;
- rispettare le norme di sicurezza;
- non manomettere in alcun modo gli apparati;
- non sostituire la dotazione con altre apparecchiature o dispositivi tecnologici;
- non utilizzare collegamenti alternativi o complementari;
- non consentire ad altri l'utilizzo della dotazione;
- effettuare la pulizia periodica (almeno semestrale) del dispositivo in uso, ivi compresi schermi, scocca e tastiera, utilizzando prodotti idonei.

L'eventuale malfunzionamento o danneggiamento degli strumenti informatici deve essere tempestivamente comunicato all'Ufficio segreteria.

È responsabilità di tutto il personale che a vario titolo presta attività lavorativa presso il Comune di Coccaglio, applicare puntualmente le regole contenute nelle presenti disposizioni**,** così come tutte le altre regolamentazioni aziendali vigenti, nonché le istruzioni fornite dai propri Responsabili.

In generale, chiunque ravvisi nell'ambito delle proprie mansioni lavorative dubbi o incertezze circa:

- l'applicazione delle istruzioni ricevute;
- il manifestarsi di nuove esigenze tecniche o organizzative che potrebbero migliorare lo svolgimento delle operazioni affidate;
- malfunzionamenti di strumenti elettronici;
- eventuali perdite di dati;
- violazioni di dati personali;
- incidenti che potrebbero compromettere la sicurezza dell'Ente
- le corrette modalità di utilizzo degli applicativi software;

deve segnalarlo tempestivamente all'ufficio Segreteria.

Art. 4 – Regole per l'uso dei dispositivi informatici

Il computer o eventualmente altro *device* mobile affidato al lavoratore è uno strumento di lavoro. Ogni utilizzo improprio, non inerente all'attività lavorativa può contribuire a creare disservizi anche agli altri utenti, nonché minacce alla sicurezza informatica.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Amministrazione mediante virus, malware o mediante ogni altro software aggressivo, quali l'apertura di messaggi di posta elettronica e dei relativi allegati di provenienza sospetta o non conosciuta e affidabile; la navigazione su siti web per ragioni non riconducibili all'attività lavorativa e così via.

Non è consentito modificare la configurazione impostata sul proprio computer portatile o eventualmente altro *device* mobile, nonché installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, ecc.) esterne agli strumenti in dotazione se non fornite dall'ente e solo per esigenze di servizio, autorizzate dall'Ufficio segreteria che provvederà materialmente all'installazione.

Non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

L'Ufficio Segreteria supporta il servizio di assistenza agli utenti, avvalendosi di personale specializzato, sia esso personale dipendente dell'Amministrazione stessa, sia personale esterno.

È buona regola la periodica pulizia degli archivi delle unità di rete, dell'hard-disk della propria postazione di lavoro e della casella di posta, con cancellazione di file ed e-mail obsoleti e inutili, ed evitando la duplicazione dei dati archiviati.

Art. 5 – Postazioni di lavoro

Gli strumenti informatici messi a disposizione del lavoratore (ad esempio, computer desktop/ portatile, notebook, smartphone, accessori, *software*, ecc.) sono di proprietà dell'Amministrazione. Il lavoratore deve custodire e utilizzare gli strumenti informatici, Internet, la posta elettronica e gli altri servizi informatici e telematici in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

Ogni dipendente che, per qualsiasi motivo, lasci incustodita la propria postazione di lavoro è tenuto a bloccare l'accesso al computer stesso o spegnere fisicamente l'apparato in questione.

Ogni utente è responsabile della custodia dei dati di lavoro presenti sulla propria postazione di lavoro informatica. Gli utenti hanno cura di conservare copia della documentazione di lavoro nelle aree condivise predisposte.

Ai sensi dell'art. 51 comma2 del CAD, riguardante la "politica di scrivania pulita", le PA sono obbligate ad adottare un insieme di procedure finalizzate a garantire la sicurezza delle informazioni riservate e sensibili. Tutti i dipendenti sono tenuti a mantenere una scrivania pulita e ordinata quando non sono in ufficio, rimuovendo la documentazione al fine di ridurre il rischio di accesso alle informazioni riservate da parte di personale non autorizzato o esterni. Le postazioni di lavoro debbono essere bloccate da password e non accessibili in assenza del dipendente. L'obiettivo è di ridurre il rischio di perdita di dati e proteggere l'organizzazione da potenziali violazioni della sicurezza.

Il personale sistemistico e tecnico-informatico incaricato della gestione e della manutenzione dei componenti del sistema informatico, può accedere alle postazioni di lavoro anche con strumenti di supporto/assistenza e diagnostica remota, per effettuare interventi di manutenzione preventiva e correttiva, richiesti dall'utente, oppure in caso di oggettiva necessità, a seguito di rilevazione di problemi tecnici sulla postazione. Gli operatori di norma non accedono ai dati di lavoro, a meno che l'intervento richiesto non sia focalizzato su questi ultimi, e comunque esclusivamente alle componenti hardware/software strettamente necessarie alla risoluzione della problematica e sono tenuti rigorosamente al rispetto del segreto d'ufficio e delle norme vigenti sulla *privacy*.

Sulle postazioni di lavoro in dotazione al dipendente agile l'Amministrazione esegue scansioni pianificate allo scopo di verificare l'eventuale presenza di codice maligno da porre in quarantena.

È proibita la modifica manuale, da parte dell'assegnatario, **dell'indirizzo di rete IP** attribuito (qualora sia statico) o del **nome host** della postazione in dotazione. Analogamente è vietata la creazione di sistemi operativi e macchine virtuali coesistenti con quelle assegnate per gli utilizzi non inerenti al contesto lavorativo. Non è permesso disinstallare o manomettere i software caricati sul sistema operativo ed in particolare i software necessari per il monitoraggio e la protezione dello stesso o della rete internet (quali antivirus o firewall).

È fatto altresì divieto assoluto di modificare autonomamente la configurazione standard della postazione, sia sotto il profilo hardware che sotto il profilo software senza l'esplicita e documentabile autorizzazione del Responsabile.

Nello svolgimento dell'attività lavorativa in "Modalità Agile", è obbligatorio utilizzare sempre gli strumenti di accesso sicuro messi a disposizione dall'Ente secondo le indicazioni fornite all'atto della consegna.

Art. 6 – Credenziali

Al dipendente sono attribuite le proprie credenziali di autenticazione per l'accesso alla postazione di lavoro o ai servizi informatici dell'Amministrazione. Di regola le credenziali in questione sono quelle già possedute dal dipendente per ragioni d'ufficio.

Ogni individuo è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali, le quali sono incedibili.

Per l'utilizzo dei servizi informatici resi disponibili dall'Amministrazione mediante pc portatile, il dipendente accede mediante VPN SSL (*Virtual Private Network*) e un sistema di autenticazione forte a doppio fattore.

Il dipendente dopo il collegamento alla VPN dell'Amministrazione e tramite le credenziali di cui al paragrafo precedente, utilizza una propria postazione di lavoro virtuale, dotata di strumenti di *office automation*, protezione dei dati, di posta elettronica, accesso ad Internet con i relativi servizi di *collaboration*.

Art. 7 – Navigazione internet

È consentita esclusivamente l'installazione di supporti per la connessione mobile per l'accesso a Internet messi a disposizione dall'Amministrazione o da essa autorizzati. Qualunque esigenza in tal senso deve essere comunicata all'Ufficio segreteria, che ha il compito di analizzare la problematica per addivenire a una soluzione coerente con le vigenti politiche di sicurezza e integrità della rete.

L'utilizzo di Internet deve essere circoscritto agli scopi inerenti all'attività lavorativa. L'utente è direttamente responsabile dell'uso del servizio Internet, dei contenuti ricercati e visitati e delle informazioni che vi immette.

Sono applicate politiche per la sicurezza della rete di trasmissione dati attraverso sistemi di "filtraggio" dei contenuti e pagine web, i quali bloccano o quantomeno limitano la navigazione su categorie di siti ben specifiche che siano potenzialmente illegali secondo normativa vigente (quali pedofilia, gioco d'azzardo, ecc.) o comunque lesivi della dignità umana (violenza, razzismo, …). Non è consentito scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer" (dall'interno della rete all'esterno e viceversa) o sistemi di "anonymous proxy".

I dati di navigazione degli utenti, sono raccolti mediante log a norma di legge e possono essere utilizzati ma non diffusi dall'Ufficio segreteria competente in materia di sistemi informativi per il monitoraggio delle funzionalità tecniche, per la risoluzione di problematiche, per scopo di sicurezza e per raccolta di dati statistici aggregati e anonimi, aventi il fine di migliorare la qualità e la fruibilità delle informazioni e dei servizi informatici e telematici.

I log sono conservati per centottanta giorni per consentirne la consultazione alle autorità competenti in caso di abusi e poi automaticamente cancellati. In ogni caso l'accesso a tali dati è consentito esclusivamente previa richiesta formale delle autorità competenti nei casi e con le procedure previsti dalla legge vigente.

Art. 8 – Posta elettronica

La casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa; deve quindi considerarsi eccezionale l'uso della posta elettronica per finalità personali e, di conseguenza, limitato a comunicazioni brevi e a carattere occasionale, ricordando sempre che l'indirizzo non è privato, bensì dell'Ente.

A tale riguardo, il dipendente è tenuto ad adottare gli accorgimenti di seguito indicati, per garantire da un lato la riservatezza di eventuali comunicazioni personali ma al contempo la continuità dell'Ente:

- utilizzare prioritariamente le caselle mail generiche dell'ufficio, e solo per comunicazioni interne le caselle mail personali;
- cancellare gli eventuali messaggi a contenuto personale - utilizzare abitualmente le caselle di posta elettronica condivise tra più lavoratori ovvero le caselle di posta di gruppo (eventualmente affiancandole a quelle individuali);
- in caso di assenza programmata, utilizzare le funzionalità del sistema di posta per l'invio automatico di messaggi di risposta recanti le coordinate della casella di gruppo o del responsabile a cui rivolgersi.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di categorie particolari di dati, si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare la particolarità del dato;
- gli allegati siano protetti con una password di accesso (comunicata con altro canale).

Ai fini della sicurezza della rete aziendale, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o FTP ambigui o comunque non conosciuti il cui indirizzo Internet sia inserito nel corpo della mail).
Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso filtri di controllo delle estensioni di allegati (es .zip, .rar .exe, etc) e filtri di limitazione anti-spam.
Eventuali segnalazioni di mail ritenute sospette devono essere inoltrate tempestivamente all'ufficio segreteria e/o all'indirizzo email assistenza@comune.coccaglio.bs.it.

È opportuno che le mail siano accompagnate dal disclaimer *" Questa comunicazione e ogni eventuale documento allegato sono ad uso esclusivo del destinatario e contengono informazioni riservate. Il messaggio ed eventuali documenti allegati non hanno natura personale e le eventuali risposte alla presente potranno essere conosciute da più soggetti e unità operative all'interno della Comune di Coccaglio, che a vario titolo abbiano interesse ad assolvere le specifiche richieste o esigenze oggetto della comunicazione. Se non siete l'effettivo destinatario della consegna della comunicazione e se l'aveste ricevuta per errore, ci scusiamo per l'accaduto e vi invitiamo cortesemente ad eliminarla in maniera definitiva senza possibilità alcuna di recupero e di comunicare immediatamente l'accaduto ai nostri uffici. Qualsiasi modifica o distribuzione a terzi è assolutamente vietata. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale".*

Con l'occasione si rammenta che il contenuto dei messaggi inviati deve essere espresso in maniera professionale e corretto e quindi non deve contenere espressioni che possano rivelarsi offensive, razziste, sessiste, discriminatorie o volgari.

Art. 9 – Software

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus e anti malware eventualmente installato sul proprio computer.

Per evitare il grave pericolo di introdurre virus e *malware* informatici nei sistemi dell'Amministrazione, devono essere utilizzati programmi messi a disposizione e distribuiti dall'Amministrazione stessa; in particolare è vietato scaricare file e *software*, anche gratuiti, prelevati da Internet, se non attinenti alle

mansioni d'ufficio, e in questo caso comunque su espressa autorizzazione del servizio informatico o dell'amministratore di sistema, che provvederà materialmente all'installazione.

Non è consentito disinstallare o inabilitare il programma antivirus e anti malware installato, ogni eventuale malfunzionamento di quest'ultimo, va segnalato tempestivamente all'ufficio segreteria competente in materia di sistemi informativi.

Nel caso che il software antivirus e anti malware rilevi la presenza di un virus e/o di un malware che non è riuscito ad eliminare, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare tempestivamente l'accaduto alla struttura dipartimentale competente in materia di sistemi informativi.

Sono vietati, se non espressamente autorizzati dal Comune di Coccaglio, la duplicazione e qualsiasi forma di estensione d'uso del software aziendale, inteso sia come software prodotto direttamente dal Comune, sia come software prodotto da terzi ed utilizzato dal Comune in forza di appositi contratti di licenza d'uso.

Art. 10 – Spazio disco

Lo spazio disco, disponibile presso appositi server accessibili in rete, rappresenta una risorsa importante a supporto della condivisione di informazioni professionali dell'Ente. Vanno, di conseguenza, evitati lo "spreco" di tale spazio, l'utilizzo per scopi non attinenti ad attività lavorative e l'utilizzo per la comunicazione non protetta di informazioni riservate o tutelate dalla legge sulla privacy.

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, vengono eseguiti periodicamente i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali file distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Sulle postazioni di lavoro o sui dispositivi mobili assegnati non vengono invece effettuate operazioni di salvataggio e non devono pertanto essere salvati file aziendali, soprattutto se contengono dati personali. In caso di compromissione della postazione di lavoro e/o malfunzionamento quest'ultima potrà essere reinstallata integralmente, con la relativa perdita di tutte le informazioni in essa conservate.

Art. 11 – Dispositivi esterni

Fatte salve le politiche di salvataggio centralizzato dei dati conservati sui sistemi informatici e sulle postazioni di lavoro virtuali dei lavoratori agili, è consentito l'eventuale uso di dispositivi di backup via USB (chiavette, hard disk esterni, ecc.) forniti dall'Amministrazione, purché i dati in essi contenuti siano comunque trattati ai sensi della normativa vigente in materia di dati personali, sensibili o giudiziari, e non vengano in nessun modo ceduti a terzi, se non nel perimetro della normativa citata e del trattamento necessario ai fini procedimentali.

Ogni dispositivo magnetico di provenienza esterna all'Amministrazione dovrà essere verificato mediante il programma antivirus e anti malware prima del suo utilizzo e, nel caso venga rilevato un virus e/o malware non eliminabile dal software, non dovrà essere utilizzato.
È vietato produrre copie informatiche di documenti e dati dell'Amministrazione su dotazioni informatiche differenti da quelle messe a disposizione da quest'ultima.

AI fine di evitare di introdurre virus o pericoli similari nella rete, è raccomandato di non copiare file di provenienza incerta da supporti quali pen-drive, memorie esterne per finalità non attinenti alla propria prestazione lavorativa.

I dispositivi esterni aziendali (dispositivi di archiviazione USB, Schede SD, ecc.) possono essere utilizzati solo in via assolutamente eccezionale, per motivi strettamente connessi ad esigenze lavorative e trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto.
I supporti esterni contenenti dati particolari o comunque riservati, devono essere custoditi in armadi muniti di serratura. Tutti i supporti già contenenti dati aziendali, ma destinati all'alienazione o a diverso utilizzo o a differente assegnatario, devono essere trattati in sicurezza, procedendo a seconda del caso con la formattazione o con la distruzione sicura, al fine di evitare che il loro contenuto possa essere recuperato dopo la cancellazione dei file da terzi non autorizzati.

Art. 12 – Policy per gli interventi di sicurezza e controlli

Il servizio competente in materia di sicurezza informatica determina le specifiche tecniche minime e di sicurezza degli strumenti messi a disposizione del dipendente.

Il personale incaricato che opera con funzioni di monitoraggio della sicurezza aziendale e di assistenza è autorizzato a compiere, nel sistema informatico dell'Ente, interventi tecnici e/o manutentivi diretti a garantire la sicurezza e la salvaguardia del sistema (es. attività di controllo, amministrazione e backup, ecc).
Tali interventi, realizzati unicamente ai fini di garanzia della sicurezza ed estranei a qualsiasi finalità di controllo dell'attività lavorativa, possono anche comportare l'accesso ai dati trattati da ciascun lavoratore, ivi compresi: le mail di posta elettronica, i siti internet acceduti, i files dei dischi di rete e locali presenti negli archivi, file personali o programmi presenti sulla postazione di lavoro.

Il collegamento o la visualizzazione da remoto del desktop della singola postazione di lavoro, può avvenire solo previa esplicita segnalazione all'interessato. È inoltre prevista l'effettuazione di controlli atti a limitare la diffusione di malware all'interno della rete aziendale o altri problemi di sicurezza informatica.

Art. 13 – Mancata osservanza delle norme e delle istruzioni

La violazione da parte degli utenti dei principi e delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare.

Si riportano di seguito gli articoli del codice di comportamento inerenti l'utilizzo delle tecnologie informatiche.

Art. 11 - Comportamento in servizio
c.3. Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione.
Art. 11-bis - Utilizzo delle tecnologie informatiche
1. L'amministrazione, attraverso i propri responsabili di struttura, ha facoltà' di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82.

2. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è' di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.
3. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
4. Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché' l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.
5. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.