
CITTÀ DI CORBETTA

# REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

**Approvato con deliberazione della Giunta Comunale nr. 63 del 07.05.2018**

## Sommario

## Art. 1 Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Corbetta ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e della correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il Comune di Corbetta ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Inoltre le disposizioni emanate dall'Autorità del Garante, mediante il provvedimento di carattere generale del 1 Marzo 2007 (Del. N. 13 del 1/3/2007), in cui vengono definite le linee guida per l'utilizzo della posta elettronica ed Internet, impongono l'adozione di precise e definite regole per l'utilizzo di tali strumenti.

Prescrizioni e riferimenti di norma, che integrano le specifiche istruzioni dettagliate nel presente Regolamento, fornite a tutti gli utenti dipendenti e/o collaboratori del Comune, sono di carattere attuativo secondo le seguenti norme integrative:

- Decreto Legislativo 196/2003 - Testo Unico in materia di protezione dei dati personali;
- Decreto Legislativo 7 marzo 2005, n. 82 del 07/03/2005 – Codice dell'amministrazione Digitale (CAD) e successive modificazioni;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3";
- Decreto-legge 29 novembre 2008, n. 185 e successive modificazioni;
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137, Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, Disposizioni legislative in materia di documentazione amministrativa;
- D.Lgs. 518/92 sulla Tutela giuridica del software;
- L. 248/2000 nuove norme di tutela del diritto d'autore;
- Circolare nr.2/2017 – AGID;

Il Comune di Corbetta, come Ente e in qualità di Datore di Lavoro, in un'ottica di trasparenza e di correttezza, per il corretto utilizzo delle attrezzature informatiche, adotta il presente Regolamento per

disciplinare il corretto utilizzo degli strumenti di lavoro e soprattutto delle risorse informatiche in dotazione a dipendenti e collaboratori così come le misure di sicurezza idonee a garantire la protezione dei dati da esso trattati, in aggiunta alle misure di sicurezza minime, al fine di assicurare il corretto espletamento delle funzioni dell'Ente e la liceità dell'attività svolta da dipendenti e collaboratori.

Il sistema informativo del Comune di Corbetta è costituito dall'insieme del patrimonio informativo digitale e dalle strumentazioni telematiche o informatiche, che permettono l'immagazzinamento, l'elaborazione, la diffusione e la condivisione delle informazioni per vie informatiche.

Le risorse informatiche si dividono in:

a) **Hardware**: Dispositivi fisici o virtuali;
b) **Software**: Programmi informatici, software di base;
c) **Firmware**: Software per il buon funzionamento dell'hardware di cui al punto a).

Per strumentazione telematica od informatica si intende tutta la strumentazione tecnologica, hardware, software o firmware che permette l'immagazzinamento, l'elaborazione, la diffusione e la condivisione delle informazioni per vie informatiche.

Rientrano in questa categoria:

a) Elaboratori personali: Personal computer, Notebook, Netbook, ultrabook o altre denominazioni commerciali per dispositivi assimilabili;
b) Dispositivi di comunicazione portatili: Telefoni cellulari, PDA, Tablet, Smartphone o dispositivi assimilabili;
c) Dispositivi per la produzione e l'elaborazione di immagini e testi cartacei: stampanti, scanner, plotter, multifunzioni, lettori di codici a barre o assimilabili;
d) Dispositivi per l'elaborazione e lo stoccaggio dei dati: Server, NAS, SAN, memorie esterne USB o schede di memoria;
e) Dispositivi per Networking: switch, hub, access-point, bridge;
f) Dispositivi per la visualizzazione: Monitor, Videoproiettori;
g) Dispositivi per la riproduzione di documenti: Fotocopiatrici, sia digitali che analogiche;
h) Dispositivi per la telecomunicazione: telefoni fissi, fax, modem, router, gateway;
i) Dispositivi e strumentazione in genere, che consentano di produrre, trasmettere, conservare ovvero duplicare dati, in formato elettronico;
j) Strumentazione atta all'autenticazione o identificazione per altre strumentazioni informatiche sopra citate (dispositivi di firma elettronica, digitale o qualificata), business key, token Usb, smartcard, lettori relativi, tecnologia biometrica;

k) Lettori bar code e sistemi RFID, ovvero una tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti ad oggetti, animali o persone basata sulla capacità di memorizzazione di dati da parte di particolari etichette elettroniche, chiamate tag e sulla capacità di queste di rispondere all'interrogazione a distanza da parte di appositi apparati fissi o portatili, chiamati reader;
l) Lettori badge e lettori rilevamento accessi uso esclusivo dei Dipendenti ed eventualmente per gli ospiti, collaboratori esterni, che devono essere debitamente informati del loro impiego solo nell'ambito del Comune e sue pertinenze; in particolare l'utilizzo dei badge da consegnare al personale esterno è regimentato e registrato mediante apposita firma dell'ospite/collaboratore esterno su apposito Registro degli Ospiti recante data/ora ingresso-uscita con la riconsegna del badge ad egli assegnato con doppia firma comprovante sia da parte del personale del Comune che dell' dell'ospite/collaboratore esterno, dell'avvenuta registrazione della visita recante l'oggetto della medesima. (da definire chi gestisce il registro);
m) Strumentazione non fisica (programmi, software, sistemi operativi, firmware) necessaria o opzionale al funzionamento della parte fisica;
n) Dispositivi di registrazione e riproduzione audio: Impianto di diffusione audio, mixer, microfoni etc;
o) Dispositivi legati alla videosorveglianza;
p) Infrastrutture di telecomunicazione wireless secondo gli standard Wi-Fi 802.1x;
q) Sistemi per la telecomunicazione in rame e/o Fibra Ottica;
r) Centralini telefonici e loro estensioni, fisiche o software.

## Art. 2 Finalità

Il presente Regolamento disciplina:

a) le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e dei servizi che tramite la stessa rete è possibile ricevere ed offrire all'interno e all'esterno dell'Amministrazione, nell'ambito dello svolgimento delle proprie mansioni ed attività di ufficio da parte degli amministratori, dipendenti e collaboratori del Comune di Corbetta;
b) l'individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia, nonché gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione Comunale.

## Art. 3 Ambito di applicazione

Il presente Regolamento si applica ad ogni utente autorizzato all'utilizzo di strumenti informatici e all'accesso alle risorse tecnologiche del sistema informatico del Comune.

Per utente si intende:

a) ogni dipendente a tempo indeterminato o a tempo determinato del Comune;
b) ogni collaboratore e/o operatore esterno che operi all'interno del Comune e che, per svolgere l'incarico assegnato, necessita dell'utilizzo degli strumenti informatici dell'Ente, sia in modo parziale che globale, debitamente autorizzato;
c) ogni Amministratore o Consigliere Comunale.

Per meglio specificare, ai fini del presente regolamento, i ruoli previsti nel sistema informativo comunale sono i seguenti:

a) "TITOLARE": si intende l'Ente Comune di Corbetta cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati, ivi compreso il profilo della sicurezza;
b) "AMMINISTRATORE DI SISTEMA": (art. 1, lettera c del DPR 318 del 28 luglio 1999 e s.m.i) si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico.

   Può essere nominato AMMINISTRATORE DI SISTEMA un dipendente, un collaboratore o una Società esterna che:

   - abbia ricevuto nomina con atto scritto ed apposito da parte dell'Amministrazione per ricoprire tale ruolo;
   - abbia le competenze tecniche per gestire le impostazioni di sicurezza del Sistema Informatico;
   - abbia almeno un set di credenziali per l'accesso ad uno o più sistemi hardware, software o firmware dotato di privilegi di sicurezza adatti a modificare impostazioni di sicurezza, impostazioni di funzionalità, eseguire aggiornamenti, modificare o eliminare altri set di credenziali utente, nel livello di accesso o nei contenuti anagrafici;

   È possibile nominare più di un amministratore di sistema, o delegare ad un singolo amministratore le funzionalità per amministrare un solo aspetto dei sistemi hardware, software o firmware.

c) "RESPONSABILE DEL SERVIZIO SISTEMI INFORMATIVI": si intende il soggetto che, per collocazione funzionale, esperienza, capacità e affidabilità assume il compito di garantire il rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza e, di concerto con l'Amministrazione Comunale, traccia le linee generali del

funzionamento di tutti gli uffici del comune collegati al sistema informativo comunale. Compete al responsabile del Servizio Sistemi Informativi la scelta del "sistema" software da adottare, di concerto con le linee stabilite dall'Amministrazione comunale, Il Responsabile del servizio Sistemi Informativi è anche custode delle password dell'intero Sistema informativo Comunale;

d) "INCARICATO DEL TRATTAMENTO": si intende il soggetto che è stato autorizzato dal titolare o dal responsabile a compiere operazioni sui dati cui ha accesso.

## Art. 4 Definizioni

Ai fini del presente Regolamento si definiscono:

Le tipologie di apparecchiature elettroniche e telematiche in:

- Client: Elaboratore individuale che non si occupa di condividere le proprie risorse con altri client;
- Server: Elaboratore che principalmente si occupa di offrire le proprie risorse agli altri utilizzatori (client);

La collocazione dei dati sugli elaboratori in:

- locale: i dati sono posizionati sulle risorse locali dell'elaboratore.
- in rete: i dati sono posizionati in risorse che non sono sull'elaboratore, ma in rete locale (LAN)
- in Cloud: i dati sono posizionati su server che non sono in rete locale, ma su posizioni accessibili solo tramite collegamenti a Internet o Sistema Pubblico di Connettività (SPC);

Le finalità del trattamento dei dati in:

- personale: i dati sono stoccati, elaborati o trattati a titolo esclusivamente personale dall'utente del sistema.
- professionale: i dati sono stoccati, elaborati o trattati in merito ad una o più attività del Comune;

Le tipologie dei dati, come da articolo 4, comma 1 del Decreto Legislativo 30 giugno 2003, n.196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" in:

a) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
b) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
c) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

d) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

## Art. 5. Strumentazione Informatica o telematica

La dotazione strumentale, informatica o telematica, ed i relativi programmi e/o applicazioni affidati all'utente, sono costituiti da strumenti di lavoro di proprietà o in uso del Comune di Corbetta, e pertanto:

a) deve essere custodita in modo appropriato;
b) deve essere utilizzata solo per fini professionali e non per scopi personali, tanto meno per scopi illeciti;
c) deve essere prontamente segnalato al Servizio Sistemi Informativi il furto, il danneggiamento o lo smarrimento di tali strumenti.

Eventuali malfunzionamenti di una o più apparecchiature devono essere segnalati al Servizio Sistemi Informativi in maniera tempestiva ed esclusivamente attraverso un sistema di ticketing.

Il personale incaricato della gestione e della manutenzione del Sistema Informativo Comunale può, in qualsiasi momento, accedere ai personal computer (anche con strumenti di supporto, assistenza e diagnostica remota), per manutenzione preventiva e correttiva, previo accordo con l'utente, il quale dovrà consentire l'abilitazione telematica e potrà verificare le operazioni eseguite durante la connessione.

La manomissione, anche parziale e non autorizzata di una qualunque delle componenti indicate nell'art.1, è da configurarsi come manomissione di un bene di proprietà del Comune.

Il Servizio Sistemi Informativi si occupa della manutenzione dell'hardware e dei software esistenti nell'Ente, avvalendosi, se necessario di fornitori esterni, e secondo le disposizioni contenute nel contratto di affidamento in essere e autorizza i relativi contratti di manutenzione ed assistenza, coordinando gli eventuali interventi e verificandone l'esatta applicazione, nel rispetto della normativa vigente.

Le procedure per la manutenzione si ispirano a principi di economicità, efficienza e funzionalità. Il responsabile del servizio Sistemi Informativi viene nominato dal Sindaco, o da un suo delegato e deve

riferire al Sindaco (titolare) o al suo delegato sull'andamento e sulla produttività del Sistema Informativo Comunale.

Le richieste di assistenza dovranno pervenire al Servizio Sistemi Informativi esclusivamente attraverso l'apposito sistema di ticketing; le segnalazioni dovranno contenere la descrizione dell'anomalia (guasto riscontrato, il nominativo del richiedente, l'ufficio di appartenenza) e qualsiasi informazione utile per il successivo intervento dell'Amministratore di sistema o del personale che concorre alla gestione dei Sistemi Informativi.

In caso di furto di qualsiasi componente facente parte della strumentazione informatica e telematica è onere dell'utente finale, o del Responsabile del settore di appartenenza, effettuare denuncia alle autorità competenti e far pervenire al servizio Sistemi Informativi copia della denuncia.

E' responsabilità del Responsabile del Settore a cui appartiene il Servizio Sistemi Informativi compartecipare al processo di gestione della sicurezza informatica e collaborare alla verifica del coerente utilizzo delle risorse assegnate ed evitarne sia l'uso improprio, che l'accesso da parte di personale non autorizzato.

L'improprio utilizzo di una parte del parco hardware e software rilevata da un Amministratore di Sistema o dal personale che concorre alla gestione dei Sistemi Informativi, comporta la segnalazione, tramite relazione scritta alla posizione organizzativa competente per l'Informatica. La posizione organizzativa responsabile del settore ove si è verificato l'utilizzo improprio valuterà se e come procedere con eventuali ulteriori azioni correttive o sanzionatorie secondo il codice disciplinare dei dipendenti in vigore presso l'Ente.

## Art 6. Utilizzo del Personal Computer

Il Personal Computer è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Il Personal computer viene assegnato all'utente in relazione alle funzioni svolte.
Ciascuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minaccia alla sicurezza.

Allo scopo di evitare il grave pericolo di introdurre programmi malevoli (malware in genere, virus informatici, spyware, adware, trojan, worms etc.) , di alterare la stabilità delle applicazioni

dell'elaboratore e, per esteso, della rete intera, e di incorrere in violazioni delle norme per la tutela dei diritti d'autore:

a) non è consentito installare programmi sprovvisti di licenza per l'utilizzo, sia questa a titolo oneroso o gratuita se non autorizzati, dal Servizio Sistemi Informativi del Comune, in particolar modo giochi o altri programmi non attinenti all'attività lavorativa;
b) non è consentito utilizzare strumenti software e/o hardware atti ad intercettare l'attività professionale, falsificare, alterare o sopprimere, il contenuto di comunicazioni e/o documenti informatici dei quali non si ha la titolarità del trattamento;
c) il Servizio Sistemi Informativi, con cadenza semestrale, aggiornerà l'elenco delle risorse infrastrutturali (hardware e software) dell'Ente;
d) non è consentito lo scarico, l'utilizzo e l'installazione di strumenti atti all'annullamento e al disarmo di protezioni informatiche di programmi o dati;
e) non è consentito modificare le configurazioni impostate sulle postazioni di lavoro o sui dispositivi informatici o elettronici in uso, senza preventiva autorizzazione del Servizio Sistemi Informativi del Comune;
f) è vietato rimuovere, inserire, danneggiare deliberatamente o asportare componenti hardware. E', altresì vietata la connessione di apparecchiature periferiche interne o esterne e l'utilizzo di memorie di massa esterne, salvo approvazione del Servizio Sistemi Informativi del Comune;
g) non è consentita l'installazione e la connessione sulle postazioni di lavoro di mezzi di comunicazione propri (come ad esempio modem, dispositivi bluetooth e similari) senza preventiva autorizzazione del Servizio Sistemi Informativi del Comune;
h) non è consentita la memorizzazione, l'elaborazione, la riproduzione, di documenti informatici, immagini o altre informazioni di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o non consone all'attività lavorativa;
i) non è consentita l'attivazione della password di accensione (B.I.O.S.), senza preventiva autorizzazione da parte del Servizio Sistemi Informativi del Comune;
j) tutti i dati di provenienza incerta o sospetta ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del Servizio Sistemi Informativi del Comune;
k) i dati presenti localmente su ciascuna postazione di lavoro NON saranno sottoposti a procedure di salvataggio o conservazione;
l) il Personal Computer deve essere spento alla conclusione della propria giornata lavorativa, salvo contraria indicazione, prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare 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. In ogni caso deve essere

attivato il programma salvaschermo, deve essere stata eseguita la disconnessione dell'utente o il blocco della postazione e la relativa password di protezione;

m) la connessione di apparecchiature periferiche (scanner, hard disk ecc.), interne o esterne ai sistemi deve essere concordata con il Servizio Sistemi Informativi del Comune;
n) è vietato l'utilizzo di memorie di massa esterne (CD, DVD, memorie USB) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus. Eventuali eccezioni devono essere concordate con il Servizio Sistemi Informativi del Comune;
o) non è consentito l'utilizzo per scopi personali delle webcam integrate nei Pc o ad esse connesse, e relativi software di gestione immagini-filmati, se non espressamente autorizzati dal Responsabile dei Sistemi Informativi o da chi ne fa le veci;
p) non è consentito l'utilizzo per scopi personali di microfoni integrati nei Pc o ad essi connessi, e relativi Software di gestione per le registrazioni di qualsivoglia contenuto, più espressamente registrazioni ambientali o registrazioni personali o in gruppo, se non espressamente autorizzati dal Responsabile dei Sistemi Informativi o da chi ne fa le veci;
q) costituisce buona regola la pulizia periodica (almeno ogni 6 mesi) degli archivi, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare, un'archiviazione ridondante;
r) la tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare, con frequenza opportuna, i salvataggi su supporti dichiarati idonei dal Servizio Sistemi Informativi del Comune.

.

La dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree deve essere concordata con il Responsabile del Servizio Sistemi Informativi, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del Responsabile del Servizio Sistemi Informativi.

E' competenza del Responsabile del Servizio Sistemi Informativi del Comune verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Agli utenti incaricati del trattamento dei dati sensibili è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CD Rom, Nastri) quando gli stessi non sono più utilizzati, al fine di rendere irrecuperabili i dati in essi contenuti. Ai sensi del Dlgs 196/03 è fatto divieto di

divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'Ente se non disciplinate da appositi protocolli di intesa.
Gli incaricati del trattamento dei dati sensibili devono:

- garantire adeguate posizioni fisiche delle attrezzature, per consentire i corretti flussi d'aria
- evitare gli assorbimenti di eccessiva umidità, ingresso di polvere o altri detriti dalle prese d'aria
- mantenere le apparecchiature sollevate dalle pavimentazioni, evitando l'accumulo di polvere e l'accidentale ingresso di liquidi o solidi
- spegnere le strumentazioni, quando il loro servizio non è richiesto.

Qualora l'accensione e lo spegnimento siano d'intralcio al corretto utilizzo della strumentazione, attivare la modalità risparmio energetico o "stand-by", consentendo così alle apparecchiature di non utilizzare funzioni non richieste al momento, riducendo la dissipazione termica, lo stress da utilizzo e prolungandone la vita.

La "rottamazione" di un personal computer o di un dispositivo elettronico deve avvenire secondo quanto previsto dal provvedimento del Garante sulla privacy.
La semplice cancellazione dei file o la formattazione dell'hard disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.
Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- preventivamente, con tecniche di memorizzazione sicura;
- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con la demagnetizzazione (degaussing), che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

## Art. 7. Utilizzo della rete del Comune di Corbetta

Possono accedere alla rete del Comune di Corbetta tutti i dipendenti, gli amministratori, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione. Questi ultimi devono essere in possesso di sistemi hardware e software "trusted", ovvero che abbiano i requisiti minimi di software Antivirus, software firewall e di hardware privo di ogni vulnerabilità per non cagionare gravi disservizi all'espletamento delle funzioni delle parti coinvolte. Il Comune si riserva di autorizzare tramite il Responsabile del Servizio Sistemi Informativi, di concedere o meno l'autorizzazione per il collegamento alla rete comunale.

Ogni postazione informatica che ha accesso alla rete comunale e ogni utilizzatore di postazione è dotato, dal Servizio Sistemi Informativi, di almeno un set di credenziali (Nome Utente e Password) che gli consentono l'accesso al Dominio, secondo quanto indicato all'articolo 9 – Gestione Account Utente e dispositivi di autenticazione

Le cartelle di rete sono condivise su server a disposizione dei vari settori, servizi ed Uffici. Ogni Settore/Servizio/Ufficio avrà uno spazio la cui dimensione è limitata e determinata dal Servizio Sistemi Informativi, in funzione delle rispettive esigenze, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e tipologia di documenti trattati.

Il Servizio Sistemi Informativi provvederà quotidianamente ad effettuare una copia di backup dei dati presenti nelle unità di rete, garantendo così la disponibilità, l'accessibilità, l'integrità dei dati in caso di smarrimento, dolo volontario e non, intrusione malevole, fatto salvo eventi riconducibili allo "Zero Day" ovvero non ancora di conoscenza dei Vendors di Hardware e Software e come tali non contrastabili nell'immediato.

Le cartelle di rete sono aree di condivisione di documenti strettamente istituzionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere allocato, nemmeno per brevi periodi, in queste unità, in particolare:

a. file di tipo multimediale (audio e video) che non hanno attinenza con l'attività lavorativa;
b. file di tipo grafico che non hanno attinenza con l'attività lavorativa;
c. file di tipo fotografico che non hanno attinenza con l'attività lavorativa;
d. qualunque altro file non pertinente e non appartenente, prodotto dai software autorizzati, e se del caso comunque a discrezione del Responsabile dei Sistemi Informativi

Nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, il Responsabile del Servizio Sistemi Informativi ha la facoltà di procedere alla rimozione di ogni file o applicazione, nonché inibire temporaneamente l'accesso alle cartelle di rete interessate.

E' vietato collegarsi alla rete comunale utilizzando mezzi propri come, ad esempio, PC portatili, ed assimilabili per natura ed al di fuori degli Assets presenti nell'Inventario delle Risorse Informatiche del Comune, senza esplicita autorizzazione del Servizio Sistemi Informativi.

Particolare attenzione deve essere prestata alla duplicazione dei dati sui Servers, con riferimento alle unità e ai volumi di pertinenza, evitando l'archiviazione ridondante.

E’ vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p.).

E’ vietato usare l’anonimato o servirsi di risorse che consentano di restare anonimi sulla rete

Il Responsabile del Servizio Sistemi Informativi predisporrà una procedura di monitoring sulla rete e sui devices ad essa connessi con lo scopo di proteggere, mitigare ogni eventuale rischio; tale procedura sarà oggetto di comunicazione laddove sarà necessaria e potrà comportare una richiesta di fermo delle attività lavorative per approfondire, valutare le eventuali azioni da intraprendere**.**

L’Amministrazione provvede a nominare il “custode delle password” che può coincidere con il Responsabile del servizio Sistemi Informativi e che dovrà custodire tutte le password chiuse in buste sigillate, in modo sicuro.

In caso di cessazione del rapporto di lavoro, l’account individuale del dipendente verrà immediatamente dismesso.

E’ compito del servizio Risorse Umane aggiornare le variazioni della dotazione organica, informando, tempestivamente, il Servizio Sistemi Informativi affinchè possa predisporre la creazione, modifica e/o cancellazione degli account, garantendo, comunque, la continuità del servizio e la sicurezza dei dati.

## Art. 8. Utilizzo delle stampanti di rete

L’utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente all’espletamento dei compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, privilegiando altresì soluzioni operative che mirino al risparmio, privilegiando innanzitutto l’utilizzo di carta riciclata con stampa fronte retro, nonché soluzioni operative che mirino ad evitare l’utilizzo di carta (memorizzazione di documenti scansionati e comunicazione via mail) nell’ottica delle direttive inerenti alla digitalizzazione della Pubblica Amministrazione. Qualunque stampa non potrà che essere prodotta da Software autorizzati. È cura dell’utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni e non. In caso di necessità la stampa in corso può essere cancellata.

## Art. 9. Gestione Account Utente e dispositivi di identificazione

L'account è costituito da un codice identificativo personale (username o user id) e da una parola chiave (password).

Si distinguono account di accesso alla rete e account di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:

a) di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete
b) gestionali, per l'accesso alle applicazioni gestionali a utenti che, per motivi di servizio, ne devono fare uso

La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Le password dovranno avere le seguenti caratteristiche:

- lunghezza minima 10 caratteri
- caratteri di tipo alfanumerico, una lettera minuscola e una lettera maiuscola ed un carattere speciale (? / ! - _ ecc.)
- validità 90 giorni

Si consiglia di utilizzare password non riconducibili a:

- nome o cognome proprio o di un collega o di un familiare
- identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo
- date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione

Va inoltre tenuto conto che:

- dopo la scadenza, potrà essere riutilizzata la medesima password solo dopo sei (6) rinnovi consecutivi
- in caso di inserimento di una password errata è possibile effettuare fino a tre tentativi dopodiché l'utenza viene bloccata

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle password, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Titolare o persona dalla stessa incaricata.

Il Servizio Sistemi Informativi deve essere contattato immediatamente in caso di:

a) Sospetto di Furto di identità digitale (diffusione di credenziali utente)
b) Comportamenti anomali del sistema (lentezza improvvisa ed eccessiva nel funzionamento)
c) Posta elettronica non desiderata o risposte non attese

L'Amministratore di Sistema o il Responsabile del Servizio Sistemi Informativi, qualora non coincidessero, è in grado di modificare le password di accesso alle caselle di posta elettronica, software applicativi ed accesso al Dominio.

L'utente che, al ritorno da un periodo di assenza, dovesse riscontrare che la sua password è stata modificata, può chiederne conto al Servizio Sistemi Informativi , il quale provvederà a fornire le spiegazioni del caso; si precisa la liceità di tale operazione per la garanzia del buon funzionamento di tutti i servizi ed il monitoring obbligatorio per evitare intenti malevoli da qualsivoglia sorgente;

E' vietato all'utente memorizzare sul Sistema Informatico Comunale dati personali o sensibili (riferimento al Dl.gs 196 del 30/06/2003 "Codice in materia di protezione dei dati personali") non attinenti alla propria attività lavorativa;

L'uso di sistemi di identificazione tramite certificato, PIN e SPID sono ammessi ai sensi del Codice dell'Amministrazione Digitale.

Attualmente, fatto salvo norme in divenire, i dati biometrici trattati dal Comune di Corbetta riguardano solamente le impronte digitali dei cittadini che richiedono la Carta di identità elettronica, con riferimento alla Circolare 31 marzo 2017, n. 4 del Ministero dell'Interno

L'uso di sistemi di identificazione biometrica, ovvero dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici, sono ammessi solo se:

- l'interessato ha prestato il proprio consenso esplicito,
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale,
- il trattamento è necessario per tutelare un interesse vitale dell'interessato,
- il trattamento è effettuato nell'ambito delle sue legittime attività,
- il trattamento riguarda dati personali resi manifestamente pubblici.

## Art. 10. Utilizzo dei supporti magnetici, ottici, chiavette, usb

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, dischi rigidi, ovvero hard disk) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del Disciplinare Tecnico D.lgs 196/2003). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione, o manipolarne il contenuto ai fini di falsificazione e danneggiamento doloso per scopi impropri.

In caso di dismissione, per evitare problemi di sicurezza, questi supporti dovranno essere consegnati al Responsabile del Servizio sistema informatico così da permettere una loro corretta distruzione, operazione che verrà tracciata in apposito Registro-Inventario, recante identificativo univoco, laddove possibile, data dell'avvenuta distruzione, operatore che ha eseguito l'attività in oggetto.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in armadi ignifughi chiusi a chiave o in cassaforte.
Non è consentito leggere, scaricare files e/o programmi contenuti in supporti magnetici/ottici/usb non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Servizio Sistemi Informativi.

## Art. 11 Utilizzo di Personal Computer portatili

L'utente è responsabile del Personal Computer portatile assegnatogli dal Responsabile del Servizio Sistemi informativi e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Oltre a quanto sopra detto, particolare diligenza deve essere posta dall'utente di PC portatili utilizzati in ambienti esterni all'Amministrazione (es. propria abitazione), sia sotto il profilo della protezione dell'apparecchiatura, sia sotto il profilo della sicurezza dei dati in essa contenuti.

Ai Personal Computer portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in rete.

I Personal Computer portatili e ogni apparecchiatura elettronica ceduta in uso dal Comune di Corbetta al dipendente, devono essere custoditi con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura del Responsabile del Servizio Sistemi Informativi. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN, fatto salvo i membri dell'ufficio dei Sistemi Informativi e del personale preventivamente autorizzato in base a giustificate necessità.

## Art. 12 Uso della posta elettronica

A tutto il personale amministrativo del Comune viene assegnata una casella di posta elettronica personale, nella forma *nome.cognome@comune.corbetta.mi.it*: Inoltre, vengono assegnate caselle istituzionali ai responsabili di servizio e di settore.

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

È fatto divieto di utilizzare le caselle di posta elettronica dell'Ente *……@comune.corbetta.mi.it* per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Non è consentito l'invio o la ricezione di messaggi con allegati di dimensione superiori a 25 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione.

Se un file supera i 25 MB, l'attuale servizio di posta elettronica gestito da Google, Gmail, aggiunge automaticamente un link di Google Drive nell'e-mail, anziché includerlo come allegato.

In caso di cessazione del rapporto di lavoro o collaborazione o di mandato degli amministratori, l'indirizzo di posta elettronica individuale dell'interessato viene immediatamente disattivato e rimosso.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e con allegati di grandi dimensioni.

E' vietato utilizzare l'indirizzo delle caselle di posta elettronica istituzionale e personale per l'invio o la ricezione di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione

E' previsto uno spazio di archiviazione massimo per ciascuna casella pari a 30 GB MB. E' buona norma non superare il 70-80% del predetto spazio.

Il Servizio Sistemi Informativi del Comune, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà di monitorare lo spazio di archiviazione occupato dalle caselle di posta elettronica sul server e informare gli utilizzatori circa l'opportunità di liberare spazio.

L'utilizzo di credenziali di altri utenti per l'accesso alla posta elettronica personale è una violazione del presente regolamento, se non autorizzata dall'autorità giudiziaria o per iscritto dallo stesso utente, nel caso di posta elettronica personale, o dai responsabili di settore/servizio, per quanto riguarda la casella di posta elettronica istituzionale.

Nel caso di accesso autorizzato, l'Amministratore di Sistema provvederà al cambio delle credenziali di accesso per meglio tutelare la sicurezza del Comune e del personale tutto.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo, se non si è certi della provenienza e del contenuto, occorre darne pronta comunicazione al Responsabile del Servizio Sistemi Informativi per le corrette azioni da intraprendere sempre ai fini della Sicurezza del Comune e del personale tutto.

È vietato inviare catene telematiche (o di Sant'Antonio), detto spamming. Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Sistemi Informativi. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Saranno messe a disposizione dei singoli incaricati le funzionalità del software di gestione della posta elettronica, che consentiranno, qualora ci dovessero essere assenze programmate, di inviare, in automatico, messaggi di risposta che contengano le "coordinate" di altro soggetto o strutture del Comune di Corbetta operanti al posto del lavoratore assente.

Qualora dovesse rendersi necessario conoscere il contenuto dei messaggi di posta elettronica in caso di assenza prolungata od improvvisa e/o per improrogabili necessità legate all'attività lavorativa, l'incaricato dovrà individuare un proprio collega "fiduciario" il quale provvederà a verificare il contenuto dei messaggi. In caso di mancata individuazione sarà cura del responsabile del settore/servizio procedete a tale nomina.

Di tale attività sarà redatto un verbale ed informato tempestivamente alla prima occasione utile il lavoratore interessato.

Si evidenzia che, qualora dovessero rendersi necessari dei controlli sull'uso della posta elettronica da parte dei lavoratori, saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori. In tal senso eventuali esigenze connesse ad azioni mirate per un monitoring della Sicurezza Informatica saranno preavvisate, laddove non si riscontri l'urgenza dovuta a potenziali minacce informatiche, tale da renderne immediato l'intervento del Servizio Sistemi Informativi, che provvederà secondo le norme vigenti a tutelare il Comune ed il personale.

## Art. 13 Uso della rete Internet, dei relativi servizi e Wi-Fi

Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (fìrewall, viruswall, antivirus, proxy server, etc.).

Il Comune di Corbetta, inoltre si è dotato di una soluzione software per la riduzione dei rischi associati all'utilizzo delle applicazioni desktop, di rete e Internet da parte dei dipendenti comunali, al fine di consentire il miglioramento della produttività e della sicurezza informatica, oltre che salvaguardare le risorse IT e ridurre i rischi di responsabilità legale.

Tale soluzione permette di gestire l'accesso a Internet da parte dei dipendenti attraverso un sistema di "filtraggio e di controllo" delle richieste di navigazione, di bloccare la condivisione di file peer-to-peer, di impedire il funzionamento di programmi spia e di gestire l'utilizzo di applicazioni a elevato consumo di banda, quali, ad esempio, il download di file audio e video, e consente di salvaguardare l'immagine e le responsabilità aziendali bloccando l'accesso ai siti Internet dai contenuti discutibili o dispersivi, di mantenere alta la produttività individuale e, di conseguenza, quella generale, ma, soprattutto di evitare utilizzi eccessivi generando traffico in Internet che potrebbe ridurre la banda trasmissiva condivisa fra tutti gli utenti del Comune ed eventuali esterni autorizzati.

Qualora dovessero rendersi necessari dei controlli sui siti web visitati, saranno rispettati i principi di pertinenza e non eccedenza e saranno evitate ingiustificate interferenze sui diritti e sulle libertà fondamentali dei lavoratori. L'accesso ai dati di connessione, che comprendono data e ora della connessione, indirizzo IP del mittente e del destinatario è limitato all'Amministratore di Sistema, il quale è tenuto al rispetto delle norme in materia di protezione dei dati.

In tal senso eventuali esigenze connesse ad azioni mirate per un monitoring della Sicurezza Informatica saranno preavvisate, laddove non si riscontri l'urgenza dovuta a potenziali minacce informatiche, tale da renderne immediato l'intervento del Servizio Sistemi Informativi.

Per questi motivi il Comune di Corbetta ha provveduto ad installare un software (detto comunemente web filter) che prevenga determinate operazioni, reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato).

Il Personal Computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico e comunque l'installazione di software prelevato da siti Internet o da altre fonti, se non espressamente autorizzato dal Responsabile dei sistemi informatici.

È fatto divieto l'utilizzo di qualsiasi strumento personale (modem, dispositivi cellulari o altro) al collegamento Lan del Comune per connettersi alla rete Internet;

Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet, né attraverso servizi peer-to-peer.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dai responsabili di settore e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti, mailing-list i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

## Art. 14 Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer

b) segnalare l'accaduto al Responsabile del Servizio Sistemi Informativi.

Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici, usb, memorie di massa esterna di provenienza ignota.

L'utilizzo di ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere autorizzato dal Servizio Sistemi Informativi, previa verifica mediante il programma antivirus.

## Art. 15 Osservanza delle disposizioni in materia di Privacy

I dipendenti del Comune di Corbetta sono obbligati ad attenersi:

- alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di nomina di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato B. "Disciplinare tecnico in materia di misure minime di sicurezza" del D.Lgs n. 196/2003 (Artt. da 33 a 36 del Codice);
- alle indicazioni obbligatorie dell'Agid in ottemperanza alla Direttiva del Presidente del Consiglio dei Ministri del 1/08/2015, CIRCOLARE 18 aprile 2017 , n. 2/2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015);

- alle nuove disposizioni del REGOLAMENTO (UE) 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

(GDPR = Regolamento Generale sulla Protezione dei i Dati).

## Art. 16 Non osservanza della normativa dell'Ente

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite:

a) Nei casi in cui la violazione costituisca un grave danno economico, di immagine o crei una interruzione del servizio, anche parziale, venga riscontrata reiterazione, volontarietà, e pertanto dolo, si intraprenderanno azioni disciplinari, d'accordo con la Posizione Organizzativa competente ai sensi del Codice Disciplinare del CCNL 11/04/2008 art. 3 comma 5.
b) Nei casi in cui la violazione non costituisca grave danno economico, di immagine, né abbia creato disservizi alcuni, ma sia comunque reiterata e volontaria, il Servizio Sistemi Informativi, previa comunicazione alla Posizione Organizzativa competente, si riserva di sospendere il servizio telematico oggetto di violazione (Internet, Posta elettronica, Cellulare, etc.).
c) Nei casi in cui la violazione non costituisca grave danno economico, di immagine, né abbia creato disservizi alcuni, né sia reiterata o comunque non sia volontaria, ma sia comunque una possibile fonte di problematiche di qualunque tipo per l'Ente, Il Servizio Sistemi Informativi provvederà a far pervenire all'Area o all'utente autore della violazione, comunicazione scritta che avrà la funzione di ammonimento ufficiale. In presenza di due o più ammonimenti ufficiali, sarà considerata una violazione volontaria, e pertanto saranno adottate le misure previste dalla normativa vigente.

Il Servizio Sistemi Informativi, seguendo quanto indicato dal Garante per la protezione dei Dati Personali, non eseguirà alcun tracciamento dei dati, se non in presenza di violazioni del presente regolamento.

Del tracciamento, salvo diverse decisioni dei titolari delle Posizioni Organizzative, degli Organi dell'Ente o dell'Autorità Giudiziaria, sarà dato avviso generalizzato a tutto il personale dell'Ente, con l'invito ad attenersi scrupolosamente al presente Regolamento e alla normativa vigente. Contrariamente, verranno svolte azioni mirate alla verifica del corretto utilizzo.

## Art. 17 Regolamento specifico per apparecchiature di telefonia mobile.

### Definizioni

Si definiscono apparecchiature di telefonia mobile tutte quelle attrezzature che consentono il trasferimento di dati, voce o flussi video su reti di telefonia radiomobile quali UMTS, GSM, GPRS, HDSPA, HSUPA, TACS, EDGE, 4G, LTE o qualunque altro tipo di comunicazione radiomobile pubbliche, dotati o meno di modulo SIM o sue derivazioni o formati.

Si definisce Assegnatario, il Dipendente, Collaboratore interno o esterno, l'Amministratore o qualunque altra persona fisica, società o ente, che venga dotato di apparecchiatura di telefonia mobile.

### Criteri per l'assegnazione

L'uso di una apparecchiatura di telefonia mobile, assegnata per motivi di servizio, può essere concesso ad un assegnatario in base ad una o più delle seguenti esigenze:

a) Necessità della reperibilità fuori dalla sede abituale di lavoro
b) Necessità della reperibilità fuori dall'abituale orario di lavoro
c) Particolari esigenze tecniche di comunicazione, tra le quali servizi che non possono essere soddisfatti con impianti di telefonia fissa e/o altri strumenti, quali la posta elettronica da postazione permanente

La durata dell'assegnazione dell'apparecchiatura è limitata alla durata dell'incarico dell'assegnatario. La scadenza dell'incarico istituzionale, le dimissioni, il licenziamento, la sospensione dal servizio, comportano l'obbligo della restituzione immediata dell'apparecchiatura, della eventuale scheda SIM e di tutti gli accessori per la telefonia mobile, nel tempo assegnati. Il mancato adempimento a questo obbligo, comporterà l'addebito all'assegnatario, delle spese per il reintegro di tali beni, sostenuti dal Comune;

All'atto dell'assegnazione e della consegna degli apparati per la telefonia mobile, l'assegnatario deve essere informato dell'esistenza del presente regolamento, e deve sottoscrivere un modulo per l'accettazione delle condizioni in esso elencate.

### Responsabili del servizio

L'Ufficio competente per il procedimento e al quale devono essere inoltrate eventuali richieste è il Servizio Economato e Gare.

Le richieste di utilizzo di dispositivi di comunicazione mobile, ad esclusione di quelle per titolari di cariche istituzionali, per i quali si procede d'ufficio, dovranno essere avanzate dalla Posizione Organizzativa dell'Area interessata all'utilizzo.

**Valutazioni economiche.**

Il Servizio Economato e Gare, procede ad una attenta e continua valutazione tecnico-economica delle offerte di servizi di telecomunicazione mobile disponibili sul mercato, anche alla luce di eventuali convenzioni generali ex legge n. 488/1999.

In particolare saranno costantemente confrontati:

a) Gli obiettivi generali per i quali è stato istituito il servizio
b) Le effettive modalità di utilizzo da parte degli assegnatari
c) I relativi costi e benefici ottenuti

**Responsabilità di utilizzo.**

L'Assegnatario dell'apparato di telefonia mobile di servizio è responsabile della corretta tenuta ed utilizzo dal momento della firma della lettera di assegnazione, fino all'eventuale revoca e/o restituzione. Ogni variazione delle norme d'uso rispetto a quelle in vigore al momento della consegna sarà direttamente segnalata agli assegnatari.

Nel caso in cui un dispositivo mobile sia concesso a più utilizzatori, l'assegnatario è individuato dal titolare della Posizione Organizzativa dell'area competente. In tale caso l'Assegnatario dovrà tenere nota degli effettivi utilizzatori per tutta la durata della concessione.

**Definizione traffico Voce**

Tutte le utenze sono attivate con la modalità di traffico "ILLIMITATO", che prevede la possibilità di effettuare chiamate su tutto il territorio nazionale, ed in casi di estrema necessità, previa autorizzazione del Responsabile di Settore dell'area competente, anche all'estero.

Per particolari esigenze del Responsabile di Settore dell'area competente, che avanza richiesta per l'attivazione dell'utenza, può chiedere anche l'abilitazione ad uso con la limitazione al solo traffico aziendale. In ogni caso non sono ammesse le chiamate ad uso personale, ad eccezione di quanto specificato al comma 3.

L'uso ai fini personali dell'apparato di telefonia mobile di servizio potrà avvenire solo in caso di attivazione del profilo tariffario doppio o "Dual Billing", che tramite l'anteposizione di un codice al numero di telefono da chiamare, permette l'addebito dei costi per uso privato, direttamente sulla carta di credito o sul conto corrente dell'utilizzatore interessato.

L'attivazione della doppia fatturazione "Dual Billing" avverrà solo dopo la firma di apposita convenzione da stipularsi tra l'assegnatario dell'apparato e l'Amministrazione Comunale.

**Obblighi derivanti dall'assegnazione**

È fatto assoluto divieto di cessione a terzi sia dell'apparato, che del modulo SIM, che degli accessori. Il Responsabile di Settore dell'area competente di appartenenza può revocare l'assegnazione, sia per non corretto utilizzo che per cessazione delle condizioni iniziali delle esigenze di servizio.

L'apparato deve essere attivo e raggiungibile – anche attraverso servizi di segreteria telefonica, se le condizioni tecniche lo consentono, secondo la seguente disponibilità:

a) Per il personale tecnico amministrativo nell'orario individuale di lavoro/servizio ed in particolare, nel caso l'assegnatario sia dotato anche di un telefono fisso, in tutti i momenti di assenza, per motivi di servizio, dal proprio ufficio;
b) Per il restante personale secondo le necessità o le responsabilità dell'incarico, in accordo con il Responsabile di Settore dell'area di appartenenza;
c) Durante le fasce di reperibilità concordata con il personale.

**Verifiche sul corretto utilizzo**

L'Amministrazione potrebbe effettuare delle verifiche al fine di accertare il traffico telefonico generato.

I controlli saranno svolti periodicamente. Potranno esser chieste giustificazioni sulle fatture controllate. Gli assegnatari chiamati a rispondere potranno produrre autocertificazione che dovrà dichiarare l'utilizzo esclusivo per motivi di servizio, in caso di utenza "ILLIMITATA", salvo dover ulteriormente giustificare, in caso di specifica richiesta, le motivazioni delle chiamate.

Il controllo del traffico sarà effettuato in ogni caso quando dall'esame delle fatture si rileverà uno scostamento significativo dalla media dei consumi.

Gli addebiti ricavati dalle fatture emesse dal fornitore del servizio dovranno essere sottoscritte dal Responsabile di Settore dell'area di appartenenza.

**Traffici alternativi alla Voce**

Per particolari esigenze di servizio, il Responsabile di Settore dell'area di appartenenza, potrà proporre il traffico IP (connessione Internet) sugli apparati di telefonia mobile.

Tale autorizzazione deve pervenire al Servizio Economato e Gare. In assenza di tale autorizzazione in forma scritta, non è ammesso l'utilizzo di traffico dati sulle apparecchiature in dotazione.

Gli utilizzatori del servizio dati sono tenuti ad utilizzare il traffico dati soltanto per esigenze strettamente legate a motivi di servizio, non espletabili in altra modalità.

Il servizio di messaggistica SMS è maggiormente economico, quindi se ne incoraggia l'utilizzo, per fini di servizio, ove non sia richiesta immediatamente la risposta di un interlocutore.

Il servizio di messaggistica multimediale MMS è da utilizzarsi strettamente per esigenze di servizio, ove non ci sia modo di trasmettere i contenuti ad esso associati in maniera alternativa.

**Traffico personale**

L''accesso al servizio **"Dual Billing"** è eseguito tramite l'anteposizione di un codice numerico al numero telefonico da chiamare.
Il codice numerico sarà comunicato agli Assegnatari all'atto della comunicazione degli estremi della fatturazione personale.
È fatto obbligo, qualora si utilizzi l'apparecchiatura di telefonia mobile (per traffico VOCE, SMS, MMS) di utilizzare il servizio di cui al comma 1 del presente articolo.
In nessun caso, a causa della impossibilità della ripartizione dei costi, è possibile accedere, per motivi personali al traffico dati su contratto aziendale.
Gli assegnatari dei dispositivi di telefonia mobile, che vogliano accedere ai servizi di cui ai comma 3 e 4 dovranno sottoscrivere un contratto con il Gestore (fornitore dei servizi di telefonia mobile), per la fatturazione del traffico personale.
È possibile, se previsto dal contratto con il fornitore, la cessione di titolarità del numero di telefono:

a) Dal Comune all'assegnatario (migrazione con portabilità del numero in dismissione)
b) Dall'assegnatario al Comune (migrazione con portabilità per integrazione)

**Obblighi derivanti dallo smarrimento, furto o danneggiamento degli apparati.**

È fatto assoluto divieto di manomissione volontaria di parti interne o esterne degli apparati, alterazione di software, che si manifestino come conseguenza di azioni dolose o volontarie che rendano l'apparato non riparabile, escluso dalle condizioni di garanzia o ne rendano la riparazione non economicamente sostenibile.
Qualora si verificassero dei danni, imputabili a comportamento non adeguato dell'assegnatario, il Comune si riserva la facoltà di addebitare all'assegnatario, l'importo che il Comune stesso dovrà eventualmente sostenere per la riparazione o sostituzione dell'apparato.
L'assegnatario, in caso di smarrimento o furto, dovrà presentare denuncia alle autorità competenti, nonché trasmettere copia di tale denuncia al Servizio Economato e Gare.
La denuncia dovrà contenere i dati identificativi dell'apparato e l'identificazione degli accessori contestualmente smarriti o rubati.
Il Servizio Economato e Gare provvederà alla reintegrazione delle apparecchiature smarrite o rubate, tramite comunicazione al Gestore e all'adempimento degli obblighi prescritti dai contratti di locazione o di uso in comodato.

**Art. 18 Aggiornamento e revisione**

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dall'Ente.
Il presente Regolamento è soggetto a revisione con frequenza annuale o quando subentrano norme che ne impongono la revisione con conseguente approvazione.
Il presente regolamento viene consegnato a ciascun dipendente/utilizzatore del Comune di Corbetta. Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" (D. M. 31 marzo 1994 - Ministero per la Funzione Pubblica).
La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i responsabili, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

## Glossario dei termini tecnici e informatici

**Account**: è la coppia nome utente e relativa password per l'accesso ad uno o più servizi rilasciata da una registrazione e consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di

entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti.

**Antivirus**: tipo di software che cerca e segnala gli eventuali programmi viirus e cerca di rimediare ai danni che potrebbero compiere

**Backup**: copia di riserva di disco, di una parte del disco o di uno o più file.

**B.I.O.S.** (Basic Input Output System): Esegue test diagnostici e controlla lo stato delle periferiche collegate, raccoglie una serie di routine software per interagire con l'hardware della macchina, per esempio, la lettura dei caratteri digitati sulla tastiera, l'invio di caratteri alla stampante, l'accesso alla memoria, alle unità disco e ad altri dispositivi di inserimento (input) e di trasferimento verso l'esterno (output) dei dati.

**Black list**: elenco di siti considerati non opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.

**Database**: (Base di dati). Qualsiasi aggregato di dati organizzati in campo (colonne) e record (righe).

**Dominio**: in ambito informatico, un ambito di risorse controllate da uno o più macchine server denominate controllori di dominio. In particolare il dominio locale è controllato dai server locali che provvedono all'attribuzione e distribuzione di risorse, viceversa il dominio Internet è inteso come la denominazione mnemonica delle risorse, anche queste controllate da uno o più server, che possono essere locali od esterni alla rete locale. Ad esempio il dominio *corbetta.local* contraddistingue tutte le risorse che possono essere reperite internamente alla rete locale, viceversa il dominio internet *comune.corbetta.mi.it* indica uno spazio gestito da un'autority che certifica l'univocità del titolare

**Download**: registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).

**E-mail**: Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica del computer mittente e destinatario. I messaggi e i file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.

**Firewall**: insieme di software/hardware usato per filtrare i dati scambiati tra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.

**Hardware**: insieme dei componenti che costituiscono un personal computer o una periferica.

**Internet**: insieme mondiale delle reti di computer interconnesse

**Intranet**: è una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni.

**MP3**: tecnologia per la compressione/decompressione di file audio/video che consente di mantenere una perfetta fedeltà e qualità anche riducendo i file rispetto alla grandezza originale

**Password**: parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente (caratteri maiuscoli/minuscoli, numeri ecc.), assieme alla user-id.

**SIC Sistemi Informativi Comunali**: servizio che, nell'ambito dell'Amministrazione, si occupa di impostare, indirizzare e coordinare l'introduzione delle tecnoclogie informatiche nell'attività del Comune, ponendosi quale punto di riferimento tecnologico per la definizione delle strategie di evoluzione e innovazione dei Sistemi informativi.

**Software**: Insieme dei programmi che permettono il funzionamento di un computer.

**Streaming**: flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet

**Url filetring**: sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività istituzionale.

**User id**: nome utente

**Utente (User)**: chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale, sia che si tratti di un accesso remoto

**Virus**: programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi installati

**White list**: elenco di siti considerati opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.