**COMUNE DI TORTORETO**

# DISCIPLINARE INTERNO PER L'UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEI DIPENDENTI

**MAGGIO 2023**

## Art. 1: OGGETTO

Il presente disciplinare, adottato sulla base delle indicazioni contenute:

- nel provvedimento di data 1 marzo 2007 (in G.U. n. 58 di data 10 marzo 2007) del Garante per la protezione dei dati personali, riguardante il *Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori* ;
- nella Direttiva n. 2 del 26 maggio 2009del Ministro per la Pubblica Amministrazione e l'Innovazione;

ha per oggetto i criteri e le modalità operative di accesso e di utilizzo del servizio internet e di posta elettronica da parte dei dipendenti del Comune di Tortoreto e di tutti gli altri soggetti che a vario titolo operano nelle strutture del Comune di Tortoreto (lavoratori socialmente utili, collaboratori, tirocinanti, stagisti).

## Art. 2 : PRINCIPI

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del Regolamento europeoGDPR n. 2016/679.

Il Comune di Tortoreto garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

1 il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (par. 5.2 del Provvedimento);

2 il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 5 GDPR) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);

3 il principio di *pertinenza e non eccedenza* (par. 6 del Provvedimento), in virtù del quale: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 5 GDPR; par. 4 e 5 del Provvedimento);

4 il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";

5 le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) e essere mirate sull'area di rischio, tenendo conto della normativa in materia di protezione dei dati personali e, se pertinente, del principio di segretezza della corrispondenza (Parere n. 8/2001, punti 5 e 12).

## Art. 3 :DEFINIZIONI

Nel presente documento si intende per :

UTENTE INTERNET: persona autorizzata ad accedere al servizio internet anche al di là dei siti istituzionali eventualmente preventivamente selezionati (white list) dall'Amministrazione comunale, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la

navigazione;
UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
WHITE LIST: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet;
BLACK LIST: elenco di siti non accessibili da nessun utente;
INTERNET PROVIDER: azienda che fornisce al Comune il canale di accesso alla rete internet;
POSTAZIONE DI LAVORO: personal computer collegato alla rete comunale tramite il quale l'utente accede ai servizi;
LOG: archivio delle attività di consultazione in rete.

## Art. 4 : MODALITÀ DI ACCESSO E UTILIZZO POSTAZIONE DI LAVORO

La configurazione dei servizi di accesso a Internet e di Posta Elettronica viene eseguita esclusivamente dai tecnici del Servizio Informatica, che può essere affidato a Ditta esterna all'Amministrazione. Le postazioni di lavoro sono preventivamente individuate e assegnate personalmente a ciascun dipendente; per accedere ai servizi informatici comunali dalla postazione di lavoro garantendone quindi la sua protezione, il dipendente dovrà utilizzare una password. Superato il sistema di autenticazione, il dipendente sarà collegato alla rete comunale e ad internet senza formalità.

Il dipendente, preso atto che la conoscenza della password da parte di terzi consente a questi ultimi di accedere alla rete comunale, nonché l'utilizzo dei relativi servizi in nome del titolare e l'accesso ai dati a cui egli stesso è abilitato, si impegna a:

1 non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;

2 non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;

3 conservare la password nella massima riservatezza e con la massima diligenza;

4 non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

5 mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati;

6 non salvare file audio, video e file non istituzionali di qualsiasi tipo nelle connessioni di rete su cui viene eseguito giornalmente il back-up;

7 Non installare o non utilizzare programmi di sistema, applicativi o gestionali privi di regolare contratto di licenza d'uso sottoscritto dall'Ente, salvo specifica autorizzazione in tal senso da parte del Responsabiledei Servizi Informatici;

8 Non modificare le configurazioni (in modo particolare l'identificativo in rete del proprio Pc impostato dall'Amministratore di sistema);

9 Non installare sul proprio Pc dispositivi hardware personali (modem, schede audio etc.), salvo specifica autorizzazione in tal senso da parte del Responsabiledei Servizi Informatici;

10 Mantenere il programma antivirus sempre attivo con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in tal senso è necessario fornire immediata segnalazione al proprio Responsabiledei Servizi Informatici;

11 Non utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Ente. Per ciò che concerne l'utilizzo di supporti magnetici e ottici, il dipendente deve attenersi alle seguenti disposizioni:

- Non è consentito scaricare files (programmi, archivi di dati, etc.) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- È fatto obbligo di sottoporre a controllo preventivo tutti i file di provenienza incerta o esterna, attinenti l'attività lavorativa.

Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, gli utenti sono configurati con diritti limitati, diversi da quelli di amministratore.

Qualsiasi azione svolta utilizzando il codice identificativo e/o la password sarà assegnata in termini di responsabilità all'utente assegnatario del codice. L'utente sarà civilmente responsabile di qualsiasi danno arrecato alla Amministrazione e all'internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dal presente disciplinare.

L'utente, inoltre, potrà essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della corte di cassazione.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente contratto collettivo provinciale di lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

## Art. 5 : INTERNET

Tutti i dipendenti cui è assegnata dall'Ente una postazione di lavoro possono utilizzare internet.

Il dipendente-utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

Tutti gli utenti cui è assegnata dall'Amministrazione una postazione di lavoro possono utilizzare internet, limitatamente ad una lista di siti istituzionali preventivamente individuati dall'Amministrazione (WHITE LIST) e previa identificazione con le modalità sopra illustrate (id. utente/password). La lista dei siti (WHITE LIST) sarà implementata nel tempo su richiesta dei responsabili dei servizi comunali.

L'utilizzo di internet, non limitato alla lista dei siti istituzionali, è libero per i Responsabili di settore, mentre sarà autorizzato per ogni singolo utente dal Responsabile dei Servizi Informatici, previa richiesta motivata dei Responsabili di settore.

Al fine di prevenire il rischio di utilizzi impropri della rete, l'Amministrazione comunale utilizza un sistema di filtri che impediscono l'accesso diretto a siti che sicuramente non hanno natura istituzionale (BLACK LIST).

Oltre a tale sistema, è attiva una funzione di verifica del contenuto del sito; ove tale contenuto, secondo l'impostazione di una soglia predefinita di filtri, appaia non istituzionale viene visualizzato un messaggio che avverte l'utente; per rendere disponibile la pagina sarà necessaria l'autorizzazione del Responsabile dei Servizi Informaticie l'inserimento del sito nella WHITE LIST .

Il dipendente-utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

Al dipendente-utente internet non è consentito:

1 Servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;

2 Effettuare transazioni finanziarie, operazioni di remote banking, acquisti on line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile dei Servizi Informatici;
3 Utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting, eMule, µtorrent o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza essere stati preventivamente autorizzati dal Responsabile dei Servizi Informatici;
4 Scaricare software gratuiti (freeware, shareware, public domain etc.) dalla rete, salvo casi di comprovata utilità (es: antivirus) ed in ogni caso previa autorizzazione in tal senso da parte del Responsabile dei Servizi Informaticiche, dopo aver verificato il rispetto delle condizioni di licenza, provvederà a eseguire fisicamente lo scarico in modalità sicura e consegnare il software al richiedente, facendo sì che venga installato da personale competente;
5 Utilizzare internet provider diversi da quello scelto ufficialmente dal Comune e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
6 Registrarsi a siti i cui contenuti non siano attinenti con l'attività lavorativa;
7 Partecipare a forum e/o l'utilizzo di chat se non per motivi strettamente attinenti l'attività lavorativa;
8 Usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

## Art. 6 : POSTA ELETTRONICA

L'utilizzo del servizio di posta elettronica è consentito, solo per ragioni di servizio, agli utenti identificati con le modalità precedentemente illustrate, ai quali l'Ente assegna una casella di posta personale e nominativa per il proprio ufficio.

In caso di assenza dal lavoro del dipendente-utente per brevi periodi, è a disposizione una apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

In caso di assenza non programmata o dove non sia stata attivata la procedura di cui sopra, il dipendente-utente può delegare un altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al responsabile del servizio quelli ritenuti rilevanti e per lo svolgimento dell'attività lavorativa.

Al dipendente:
1 Non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
2 Non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum, mail-list, salvo specifica autorizzazione in tal senso da parte del Responsabile dei Servizi Informatici;
3 E' vietato utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra aziendali o di azioni equivalenti;
4 E' vietato utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), messaggi tipo "catene di S. Antonio" e altre e-mails che non siano di lavoro;
5 E' vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive;
6 E'vietata l'apertura di allegati di non comprovata origine. Il ricevimento di detti messaggi deve essere tempestivamente segnalato al Responsabile dei Servizi Informatici;
7 E'vietata l'apertura di link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
8 E'vietato il download di file con estensioni: .vbs, .bat, .exe o successiva esecuzione delle

macro in esso contenute;
9 E'vietata la risposta ad e-mail pervenute da mittenti sconosciuti. Si suggerisce, nel dubbio, di cancellarle preventivamente;
10 E'vietato l'invio di allegati in formato Ms-Word (estensione .doc/docx): utilizzare in alternativa il formato PDF (estensione .pdf);
11 E'vietato l'invio e l'accettazione, anche in sola lettura, di messaggi formato html;

L'utilizzo di liste di distribuzione riservate, comunemente riunite nella- Rubrica gruppi", che permettono l'invio di e-mail a una pluralità di utenti o a tutti gli utenti, è consentito solo a determinati soggetti, su autorizzazione del Responsabile dei Servizi Informaticie previa richiesta del Responsabile di Settore.

## Art. 7 : CONTROLLI

L'Ente, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es. per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dell'art. 4, comma due dello Statuto dei Lavoratori, di sistemi che consentano indirettamente un controllo a distanza (cd. controllo preterintenzionale), e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto di quanto previsto dal paragrafo 5 del Provvedimento del Garante.

Le comunicazioni effettuate attraverso il servizio di posta elettronica interno sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte dell'Ente, dell'internet provider o da parte di altri soggetti.

L'Ente non effettua in alcun caso trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza dei lavoratori grazie ai quali sia possibile ricostruire la loro attività e che vengano svolte tramite i seguenti mezzi:

- Lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire e gestire il servizio di posta elettronica;
- Riproduzione e eventuale memorizzazione sistematica delle pagine web visualizzate dal dipendente;

  Lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;

  Analisi occulta dei dispositivi per l'accesso a Internet o l'uso della posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema.
Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.
I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Responsabile dei Servizi Informaticiper le valutazioni di competenza e riguardano:

- per ciascun sito/dominio visitato le seguenti informazioni: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
- per ciascun utente le seguenti informazioni: il numero di siti visitati, la quantità totale di dati scaricati, e le postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati in via eccezionale e tassativamente

nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- su richiesta del Responsabile dei Servizi Informaticiquando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- su richiesta del Responsabile dei Servizi Informaticilimitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura/area (rilevabile esclusivamente dai dati aggregati) e reiterato il mese successivo nonostante un necessario esplicito invito agli utenti da parte del Responsabile dei Servizi Informaticiad attenersi ai compiti assegnati ed alle istruzioni impartite.

I dati contenuti nei LOG sono conservati per il tempo necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non inferiore a sei mesi, come previsto dal Provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008.

I dati riguardanti il software installato sulle postazioni di lavoro, senza alcuna indicazione dell'utente che ha effettuato l'installazione, possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

## Art. 8 :PUBBLICAZIONE DI CONTENUTI E REALIZZAZIONE DI SITI PERSONALI

Il dipendente-utente non è autorizzato a produrre e pubblicare propri siti web. Ogni eventuale necessità di realizzare siti web personali o di struttura dovrà essere espressamente autorizzata dal Responsabile dei Servizi Informatici.

Il dipendente-utente si obbliga a tenere indenne l'Amministrazione da tutte le perdite, danni responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovessero essere subite o sostenute quali conseguenze di qualsiasi inadempimento da parte dell'utente agli obblighi e garanzie previste nel precedente paragrafo e comunque connesse alla immissione delle informazioni in internet anche in ipotesi di risarcimento danni pretesi da terzi a qualunque titolo

## Art. 9 : INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO

Il servizio di internet e posta elettronica può essere interrotto per le manutenzioni ordinarie e straordinarie; le interruzioni saranno preventivamente comunicate agli utenti, salvo casi di forza maggiore.

Ai sensi della presente informativa, l'utilizzo del servizio di accesso ad internet cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
- se è accertato un uso non corretto del servizio da parte del dipendente-utenteo comunque un uso estraneo ai suoi compiti professionali;
- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software del dipendente-utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione imputabili direttamente o indirettamente al dipendente-utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
- in caso di accesso doloso del dipendente-utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività del dipendente-utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da

parte del dipendente-utente a terzi;

- in caso di violazione e/o inadempimento imputabile al dipendente-utente di quanto stabilito nei precedenti punti.
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi del dipendente-utente.

## Art. 10 :DIFESA DAL RANSOMWARE

Il ransomware è un programma informatico dannoso ("malevolo") che può “infettare” un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, “ransom”) da pagare per “liberarli”.

E' vietato aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.

Anche se i messaggi provengono da soggetti a noi noti, è comunque necessario:
- passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli. Nel dubbio non cliccare sul link e avvisare il Responsabile del Servizio informatico;
- non aprire mai allegati con estensioni "strane" (ad esempio, allegati con estensione “.exe” sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento).

## Art. 11 :UTILIZZO SISTEMI DI VIDEOCONFERENZE

I sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica.
Si ricorda:

- di dotarsi di cuffie con microfono (per esempio anche quelle del telefono cellulare) . Questo migliora sensibilmente la qualità del segnale audio;
- di spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze;
- che nel caso ci si connetta dalla propria abitazione e non si disponga di una zona riservata è possibile utilizzare sfondi virtuali, o, se si preferisce, disattivare la videocamera;
- che nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio- video è conveniente spegnere la videocamera;
- di scollegarsi sempre al termine della videoconferenza, la stessa stanza potrebbe essere utilizzata successivamente per altre riunioni.

## Art. 12 :GLOSSARIO

**Backup**: il termine, che significa copia di sicurezza, indica l’operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.
**Chat**:(letteralmente,“chiacchierata”)èunservizioinformaticochepermetteattraversointernet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.
**Filesharing**:condivisionedifileall'internodiunaretecomune.
**Forum**: generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce

comunementeaiforumanchecomeboard,messageboard,bulletinboard,gruppididiscussione, bacheche e simili.
**Guestbook**:(letteralmente,librodegliospiti)èunserviziointerattivochepermetteaivisitatoridi un sito web di poter lasciare 'firme' e commenti.
**ID utente**: codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.
**LOG**: il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informaticaperindicarelaregistrazionecronologicadelleoperazionimanmanochevengono eseguite ed il file su cui tali registrazioni sono memorizzate.
**Mailing-list**:(letteralmente,listapercorrispondenzatraducibileinitalianoconlistadidiffusione) èunsistema organizzatoperla partecipazione di più persone in una discussione tramite posta elettronica.
**Mailspamming**:èl'inviodigrandiquantitàdimessaggiindesiderati(generalmentecommerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è internet attraverso l'e- mail.
**Password**: (in italiano: "parola chiave", "parola d'ordine", o anche "parola d'accesso") è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.
**Podcasting**: sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.
**Ransomware**:programma informatico che può "infettare" un dispositivo digitale bloccando l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli".
**Softwarefreeware**:programmisoftwaredistribuitiinmodo gratuito.
**Software peer-to-peer**: programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzatiprincipalmenteper scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti i film) spesso in violazione dei diritti d'autore.
**Stand-alone**:siriferisceadun'apparecchiaturacapacedifunzionaredasola,indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.
**Streaming**: identifica un flusso di dati audio/video trasmessi da una sorgente a una o più destinazionitramiteunaretetelematica.Questidati vengonoriprodotti man mano che arrivano a destinazione.
**Videoconferenza**: Si definisce *videoconferenza* la combinazione di due tecnologie, dove si ha l'interazione sincrona in audio, video e dati fra due o più soggetti.
**Webcast/Webcasting**: descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di webcasting) e di ascoltare o visualizzare il contenuto audio/video.