COMUNE di GUBBIO
Provincia di Perugia
c.f. e p.i. 00334990546
Affari Generali
Servizio Informatica
piazza Grande, 1 - 06024 GUBBIO – PG

DISCIPLINARE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI

CON RIGUARDO ALLA DISCIPLINA DELLA TUTELA DEI DATI PERSONALI

Linee guida dirette a definire i criteri e le modalità organizzative per l'utilizzo dei servizi di rete internet e/o posta elettronica

INDICE

CAPO I - FINALITA' - AMBITO DI APPLICAZIONE - PRINCIPI GENERALI

Art. 1 FINALITA'
Art. 2 AMBITO DI APPLICAZIONE
Art. 3 PRINCIPI GENERALI
Art. 4 AMMINISTRATORE SISTEMA

CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 5 UTILIZZO DEL PERSONAL COMPUTER
Art. 6 UTILIZZO DELLA RETE
Art. 7 GESTIONE DELLE PASSWORD E DEGLI ACCOUNT
Art. 8 UTILIZZO DEL PERSONAL COMPUTER PORTATILE
Art. 9 UTILIZZO DEI SUPORTI MAGNETICI
Art. 10 UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO
Art. 11 SOFTWARE E COPYRIGHT

CAPO III - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 12 UTILIZZO DI INTERNET
Art. 13 GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA

CAPO IV – CONTROLLI

Art. 14 CONTROLLI E RESPONSABILITA'
Art. 15 RESPONSABILITA' DEGLI UTENTI

CAPO V - AGGIORNAMENTO E REVISIONE

Art. 16 REVISIONE

CAPO VI -DISPOSIZIONI DI RINVIO

Art. 17 PROCEDURE OPERATIVE

ALLEGATO A - GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

CAPO I - FINALITÀ - AMBITO DI APPLICAZIONE – PRINCIPI GENERALI - AMMINISTRATORE DI SISTEMA

Art. 1 - Finalità

1. Le presenti linee guida sono dirette a definire le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e telematica e dei servizi che tramite la stessa rete è possibile ricevere all'interno e all'esterno dell'Amministrazione, ai fini di un corretto utilizzo degli strumenti stessi da parte di amministratori, dipendenti dell'Ente o collaboratori, consulenti, stagisti, tirocinanti e soggetti autorizzati dal Comune di Gubbio.
2. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune di Gubbio.
3. Per quanto non specificato nel presente documento è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede.
4. Resta valida in ogni caso l'assunzione di responsabilità personale per il proprio PC; in caso di dubbi, necessità di informazioni, sospetto di tentativi di intrusione ecc. l'utente deve rivolgersi immediatamente all'Ufficio Informatica.

Art. 2 - Ambito di applicazione

1. La rete del Comune di Gubbio è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.
2. Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica comunale.
3. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
4. Le presenti linee guida si applicano a tutti gli utenti interni di cui all'art. 1, comma 1, che sono autorizzati ad accedere alla rete comunale.

Art. 3 - Principi generali

1. Il Comune di Gubbio promuove l'utilizzo della rete informatica e telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi/programmi a cui ha accesso e dei dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.
3. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Ente.

Art. 4 - Amministratori di sistema

1. Si definisce amministratore di sistema il soggetto a cui è conferito, mediante specifica lettera di incarico, il compito di sovraintendere a una o più risorse informatiche dell'Ente.
2. Gli amministratori di sistema sono obbligati ad operare nel rispetto delle politiche dell'Ente in materia di sicurezza, a garantire la massima riservatezza nella trattazione dei dati personali anche desunti dal software di analisi del traffico, a mantenere riservate le informazioni relative al collegamento degli utenti fatti salvi i casi di interessamento dell'Autorità Giudiziaria a fronte di ipotesi di reato.
3. L'Ufficio Informatica, sentito il dirigente preposto, revoca l'accesso temporaneo alla risorsa informatica e di rete, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti. Potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
4. Il personale dell'Ufficio Informatica ed i suoi collaboratori possono accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell'Ente, sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

CAPO II - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 5 - Utilizzo del personal computer

1. Il personal computer (PC) 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 al dipendente, collaboratore o altra forma particolare di lavoro in relazione alle funzioni svolte. La collocazione del personal computer nella propria postazione di lavoro deve essere tale da ridurre il rischio di utilizzo a fini impropri e non legati all'attività lavorativa.
2. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico, quali l'utilizzo di supporti per la memorizzazione dei dati non sicuri e CD provenienti dall'esterno, al fine di non diffondere virus.
3. E' necessario spegnere o bloccare il personal computer al termine dell'attività lavorativa quotidiana e in caso di assenza prolungata dal proprio ufficio, al fine di evitare l'utilizzo da parte di terzi e l'indebito uso.
4. Non è possibile modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione.
5. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. E' vietata l'installazione non autorizzata di hardware che consenta l'accesso non controllato all'esterno della rete comunale (ad es. internet key, chiavi Wireless USB o modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne).
7. E' vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto di autore (documenti, files musicali, immagini, filmati e simili) di cui l'Ente non abbia acquisito preventivamente i diritti.
8. L'Ufficio Informatica ed i suoi collaboratori possono procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui singoli personal computer sia sulle unità di rete.
9. L'Ufficio Informatica ed i suoi collaboratori possono, in qualsiasi momento, accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa informazione all'interessato.
10. Tutti i dati sensibili riprodotti su supporti magnetici o su supporti cartacei devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Non è pertanto consentito lasciare incustoditi presso le stampanti documenti cartacei contenenti dati sensibili.
11. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato all'Ufficio Informatica.
12. È responsabilità del responsabile di ciascun servizio verificare il coerente utilizzo delle risorse assegnate al fine di prevenirne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.
13. Nel caso in cui ci siano problemi sui personal computer il dipendente deve inoltrare apposita segnalazione, preferibilmente a mezzo mail o in alternativa a mezzo telefono, all'ufficio Informatica per richiedere l'intervento, indicandone il motivo e le generalità dell'ufficio/dipendente richiedente.
14. Per nuove installazioni di personal computer o spostamenti degli stessi è necessario che il responsabile invii una mail all'ufficio Informatica indicando la motivazione ed in dettaglio: utente che dovrà utilizzare il personal computer, programmi eventuali da installare, mail da configurare, stampanti da collegare e risorse da condividere.
15. E' vietato, in caso di cessazione del servizio, provvedere alla cancellazione dei file personalmente, ma occorre contattare l'Ufficio Informatica.

Art. 6 - Utilizzo della rete

1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Ufficio Informatica.
2. L'Ufficio Informatica può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
3. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti da evitare un'archiviazione ridondante.

Art. 7 - Gestione delle password e degli account

1. L'account è costituito da un codice identificativo personale (username o user-ID) e da una parola chiave (password).
2. Si distinguono account di accesso alla rete e di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:
    a. account di rete, per l'accesso ai personal computer e alle risorse di rete
    b. account per l'accesso a particolari programmi e applicativi.
3. Non è consentita l'attivazione nel BIOS dei personal computer della password d'accensione, senza preventiva autorizzazione da parte dell'Ufficio Informatica. Per incrementare il livello di sicurezza l'Ente adotterà progressivamente l'utilizzo dei seguenti criteri:
    a. La password dovrà essere costituita da almeno otto caratteri che possono essere lettere (maiuscole e/o minuscole), numeri e caratteri speciali, evitando contenuti di senso logico immediato facilmente individuabili.
    b. La password sarà personale e segreta verrà cambiata periodicamente almeno ogni tre mesi.
    c. È proibito entrare nella rete e nei programmi con nomi utenti diversi dal proprio, fatto salvo quanto previsto al successivo comma 4;
    d. Non sarà consentito riutilizzare le precedenti due password.
4. In caso di assenze prolungate e programmate, qualora se ne ravvisi la necessità, il dipendente interessato deve darne comunicazione al Servizio Informatica che provvederà a delegare ad un altro dipendente l'utilizzo del proprio personal computer.

Art. 8 - Utilizzo di personal computer portatili

1. Il dirigente/responsabile del servizio, qualora ritenga necessaria l'assegnazione di personal computer portatili da utilizzare da parte del proprio personale, inoltra apposita richiesta motivata all'Ufficio Informatica.
2. L'utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
3. L'utilizzo dei personal computer portatili deve seguire le stesse regole previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
4. I PC portatili utilizzati all'esterno (convegni, riunioni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
5. Eventuali configurazioni di tipo accesso remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura dell'Ufficio Informatica. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

Art. 9 - Utilizzo dei supporti magnetici

1. Tutti i supporti magnetici riutilizzabili (DVD, CD, dischetti, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.
2. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
3. Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
4. 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 dell'Ufficio Informatica

Art. 10 - Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali, ecc.) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali e/o utilizzi eccessivi.

Art. 11 - Software e copyright

1. L'utente risponde del software installato sul computer che gli è affidato.
2. L'Ufficio Informatica provvede all'acquisto o alla regolarizzazione delle licenze necessarie per il software presente sui computer dell'Ente.
3. È vietato:
    1. distribuire software soggetto a copyright acquistato dall'Ente, al di fuori dei termini delle licenze;
    2. distribuire software che possa danneggiare le risorse informatiche, anche via e-mail;

3. accedere a dati e/o programmi per i quali non vi è autorizzazione o esplicito consenso scritto da parte dell'intestatario.

CAPO III - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 12 - Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato esclusivamente a scopi inerenti l'attività lavorativa, fatta salva la possibilità di assolvere incombenze amministrative e burocratiche, come ad esempio l'effettuazione di adempimenti on line nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari ed assicurativi, purchè tale utilizzo sia limitato al tempo strettamente necessario.
2. Sono pertanto vietati:
   - l'uso di Internet per il download di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio (ad esempio: film, musica e software);
   - l'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo.
   - l'utilizzo di qualsiasi mezzo alternativo (modem, chiavette o altro) al collegamento Lan dell'Ente per connettersi ad Internet;
   - l'accesso alla rete dall'esterno via modem o con qualsiasi altro mezzo di accesso remoto senza l'autorizzazione del responsabile della sicurezza informatica;
   - lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.
3. L'Ente provvederà ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura; in particolare viene attuato un filtraggio preventivo rispetto a siti internet o a contenuti ritenuti inequivocabilmente non inerenti l'attività lavorativa. Qualora tali sistemi di filtraggio impediscano l'utilizzo di siti o risorse utili all'attività lavorativa, il dirigente interessato deve inviare segnalazione scritta all'Ufficio Informatica.
4. I dati relativi alla navigazione in internet dai PC della rete comunale (nello specifico: Data della connessione – Ora della connessione - Indirizzo di rete del PC comunale – Indirizzo di rete computer chiamato [server o generalmente host] [es. server web, mail ecc.] – Esito della richiesta [operazione permessa/bloccata] – riferimento alla regola del firewall) sono memorizzati tramite i dispositivi sopra citati e possono essere oggetto di controllo. I contenuti delle pagine visualizzate non sono memorizzati.
5. L'utilizzo della rete internet resta assoggettato alle norme di Netiquette (insieme di regole che disciplinano il comportamento di un utente di Internet nel rapportarsi agli altri utenti attraverso risorse quali newsgroup, mailing list, forum, blog o e-mail in genere).

Art. 13 - Gestione e utilizzo della posta elettronica

1. La casella di posta elettronica individuale viene assegnata a qualsiasi dipendente che, per le funzioni svolte, è dotato di personal computer. Per particolari forme di lavoro, qualora le funzioni svolte richiedano l'uso della posta elettronica, la casella di posta elettronica individuale viene assegnata su espressa richiesta del responsabile di riferimento.
2. L'Amministrazione rende inoltre disponibili, oltre a quelli individuali, anche indirizzi di posta elettronica condivisi da più utenti. Il responsabile o suo delegato di riferimento individua un responsabile della gestione della casella di posta elettronica condivisa.
3. La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa. Gli assegnatari sono responsabili del corretto utilizzo della stessa.
4. E' fatto divieto di utilizzare la casella di posta elettronica per:
   - trasmissione di dati sensibili, salvo i casi espressamente previsti dalla normativa vigente in materia di dati sensibili;
   - trasmissione di dati confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;

- partecipazione a dibattiti, forum, o mailing-list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.

5. E' vietata l'apertura di allegati a messaggi di posta elettronica senza il previo accertamento dell'identità del mittente.
6. Non è consentito l'invio di messaggi con allegati di dimensione superiori a 50 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica di cui si avvale il Comune di Gubbio potrebbe non consentire la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate all'Ufficio Informatica che individuerà la soluzione tecnica più appropriata.
7. Qualora le funzioni svolte lo rendano opportuno è consentito l'accesso alla casella di posta elettronica individuale dall'esterno della LAN dell'Ente, anche mediante smartphone e simili, nel rispetto delle norme di protezione dei dati personali, e previa autorizzazione dell'Ufficio Informatica.
8. In caso di assenze dal lavoro, programmate o non programmate, l'interessato deve delegare un altro lavoratore a verificare il contenuto dei messaggi e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti ed urgenti per lo svolgimento dell'attività lavorativa.
9. In caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica individuale dell'interessato viene mantenuto attivo per un periodo di tempo pari a 6 (sei) mesi.

CAPO IV- CONTROLLI

Art. 14 - Controlli e responsabilità

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto dei principi di pertinenza e non eccedenza, di correttezza e di gradualità come previsto dalla normativa vigente.
2. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti. I controlli possono essere attivati dall'Ufficio Informatica a seguito di richiesta del responsabile del servizio o a seguito della rilevazione di anomalie / malfunzionamenti del sistema. Il primo controllo sarà anonimo e nel rispetto del principio di gradualità; qualora – durante un controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Ente procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente Regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
3. Il mancato rispetto o la violazione delle norme contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Art. 15 - Responsabilità degli utenti

1. L'utente non può in alcun caso modificare la configurazione di rete e non può effettuare manomissioni o interventi sulle apparecchiature o sui programmi non formalmente autorizzati dall'Ufficio Informatica, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta prestazione dei servizi.
2. L'accesso alla risorsa informatica è personale e va effettuato tramite nome utente e password di identificazione. L'accesso non può essere condiviso o ceduto.
3. Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi non espressamente e preventivamente autorizzati dall'Ente.
4. La password è personale e non cedibile o trasmissibile a terzi: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, username e comunque chiavi di accesso riservate. Se smarrite, va fatta immediata segnalazione e richiesta di sostituzione all'Ufficio Informatica, fatto salvo quanto previsto all'art. 7, comma 4.
5. Gli utenti sono obbligati a segnalare immediatamente all'Ufficio Informatica ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.
6. Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive dell'Ufficio Informatica divulgate tramite e-mail.

CAPO V - AGGIORNAMENTO E REVISIONE

Art. 16 - Revisione

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni alle presenti linee guida. Le proposte verranno esaminate dal Servizio Informatica.

CAPO VI - DISPOSIZIONI DI RINVIO

Art. 17 – Procedure operative

1. Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, oltre che alle norme del presente Regolamento, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".
2. 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 dirigenti responsabili, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

ALLEGATO A

GLOSSARIO DEI TERMINI TECNICI E INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userld e di una password, 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. Altri account servono per accedere a server e servizi vari.
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Backup	Copia di riserva di disco, di una parte del disco o di uno o più file.
Database	(Base di Dati). Qualsiasi aggregato di dati organizzato in campi (colonne) e record (righe).
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 dei computer mittente e destinatario. I messaggi e 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 in scambio fra 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.
Freeware	Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD-ROM allegati a pubblicazioni in edicola.
Hardware	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
Internet	La madre di tutte le reti di computer. È l'insieme mondiale delle reti di computer interconnesse.
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
MP3 (MPEG-4)	Tecnologia per la compressione/decompressione di file audio che consente di mantenere una perfetta fedeltà e qualità anche riducendo il file audio di ben 11 volte la lunghezza originale.
MPG (Motion Picture Experts Group)	Stabilisce gli standard digitali per audio e video.
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, assieme alla user-id.
Quicktime	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
Software	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoi ed immagini) per i computer.
Streaming	Con il termine **streaming** si intende un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
Url filtering	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 aziendale.
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	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.