

# **UNIVERSITA' DEGLI STUDI DI PERUGIA**



***LINEE GUIDA***

***PER***

***L'UTILIZZO DELLA***

***RETE INTERNET E DELLA POSTA ELETTRONICA***

**Emanato con D.R. n. 1087 del 27 maggio 2010 – Pubblicato all'Albo  
Ufficiale d'Ateneo al n. 379 il 31 maggio 2010**

## **CAPO I**

### **PRINCIPI GENERALI**

#### **Art. 1**

##### **Finalità**

1. L'Università degli Studi di Perugia, nel promuovere ai sensi dell'art. 12 del d.lgs 7 marzo 2005, n. 82 (*Codice dell'Amministrazione digitale*) 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, disciplina le misure tecniche ed organizzative poste a garanzia del corretto uso degli strumenti suddetti, disponibili presso le stazioni di lavoro di proprietà dell'Università medesima, tenuto conto delle peculiarità proprie di ciascuna struttura, della diversità dei profili di utenza autorizzata all'uso della rete, e, comunque, in ossequio alle disposizioni prescritte dalla vigente normativa nazionale.

2. Il presente regolamento, stilato in conformità alla policy di utilizzo della rete da parte del GARR e ispirato ai principi della Netiquette (*all. sub. n. 1 e 2*), è un atto dovuto e previsto dal provvedimento del Garante per la Privacy, pubblicato sulla G.U. n. 58 del 10 marzo 2007.

3. Le prescrizioni contenute in questo disciplinare possono essere integrate con ulteriori norme comportamentali che le strutture universitarie, in ragione della peculiarità delle proprie attività, potranno riservarsi di applicare per l'accesso ai propri servizi, laboratori e similari, fatta salva, in caso di disposizioni discordanti, l'applicazione del presente regolamento.

#### **Art. 2**

##### **Principi e regole comportamentali generali**

1. L'Università, quale datore di lavoro, è tenuta ad assicurare la funzionalità e il corretto impiego degli strumenti informatici di sua proprietà, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa e adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi, nel rispetto dei generali principi di proporzionalità, pertinenza, necessità e non eccedenza delle attività di controllo, applicando ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà.

2. Il dipendente è tenuto al corretto espletamento della prestazione lavorativa, assumendo un comportamento idoneo a non causare danni o pericoli ai beni mobili e agli strumenti ad essi affidati, tra i quali le attrezzature e i sistemi informatici messi a disposizione dell'Università, astenendosi dal porre in essere attività non correlate alla prestazione lavorativa, anche mediante l'utilizzo, a fini privati, di materiale o attrezzature di cui dispone per ragioni d'ufficio.

3. Sono, altresì, vietati comportamenti che possono creare un danno, anche di immagine, all'Università.

4. Il mancato rispetto o la violazione delle disposizioni contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali previste dalle vigenti normative in materia, come sancito al successivo art. 13.

### **Art. 3**

#### **Ambito di applicazione**

1. Il presente regolamento si applica a tutti i dipendenti dell'Università, nonché agli utenti espressamente autorizzati ad accedere alle risorse informatiche d'Ateneo, in ragione del proprio rapporto di lavoro, collaborazione e/o studio.

2. Tutti gli utenti a cui viene fornito l'accesso alle risorse informatiche devono essere identificati e identificabili e devono, altresì, aver previamente preso visione e accettato integralmente le norme contenute in questo documento a cui l'Università ha l'onere di dare opportuna pubblicità, con modalità analoghe a quelle previste dall'art. 7 della L. n. 300 del 20 maggio 1970 (*Statuto dei Lavoratori*).

## **CAPO II**

### **CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI**

#### **Art. 4**

##### **Utilizzo del personal computer**

1. Il personal computer è uno strumento di lavoro e il suo utilizzo deve essere finalizzato allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza del sistema informatico, quali la diffusione di virus.

2. In ogni caso, l'utilizzo del personal computer non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'Amministrazione o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

3. E' responsabilità dei soggetti- già individuati in ragione delle proprie funzioni apicali e organizzative ai sensi del D.R. 1077 del 01 giugno 2004 e successivi atti e provvedimenti- verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso da parte di personale non autorizzato.

## **Art. 5**

### **Utilizzo delle stazioni di lavoro**

1. Le stazioni di lavoro, da tavolo o portatili, sono predisposte con la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da consentirne il corretto funzionamento ai fini dell'attività lavorativa a cui la dotazione medesima è finalizzata.
2. Nessuna delle attività di configurazione e installazione a carico delle dotazioni di cui al precedente comma 1 deve pregiudicarne il corretto funzionamento.
3. La collocazione del personal computer nella propria postazione di lavoro deve essere tale da ridurre il rischio di utilizzo a fini impropri, non legati all'attività lavorativa ovvero in contrasto con le tutele previste al d.l. 30 giugno 2003, n. 196.
4. Per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti assegnati, il dipendente ha l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbiano potuto usare la postazione lavorativa.

## **Art. 6**

### **Credenziali di accesso**

1. Al fine di assicurare il corretto adempimento delle prescrizioni di cui al precedente art. 5, commi 3 e 4, l'utente è tenuto a bloccare o spegnere il personal computer in caso di sospensione o termine dell'attività lavorativa, assicurandosi di evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso.
2. Le credenziali di accesso di cui al precedente comma 1 (generalmente, nome utente e password) sono strettamente personali ed ogni attività non regolare sarà imputata al titolare delle credenziali medesime.
3. Per la disciplina riguardante l'utilizzo delle credenziali e la segretezza e tutela delle password è fatto riferimento espresso alle disposizioni contenute al d.L. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*), e, in particolare, agli artt. 4, comma 3, lett. d) e 34, nonché alla normativa regolamentare già formulata e pubblicata dall'Università.

## **Art. 7**

### **Utilizzo di personal computer portatili**

1. I criteri di assegnazione dei personal computer portatili sono contenuti nei Piani Triennali per l'individuazione di misure finalizzate all'utilizzo delle dotazioni strumentali, approvati dai competenti Organi accademici.

2. L'utilizzo dei personal computer portatili segue le stesse regole previste per i personal computer connessi in rete.

### **CAPO III**

## **GESTIONE DELLE COMUNICAZIONI TELEMATICHE**

### **Art. 8**

#### **Utilizzo di Internet**

1. Il servizio di accesso ad Internet deve essere utilizzato a fini istituzionali, per l'espletamento della prestazione lavorativa, ivi incluse le attività conseguenti all'attuazione di Convenzioni o accordi approvati dagli Organi competenti, rispettando le regole di comportamento previste nel presente regolamento, salvo i casi espressamente autorizzati dalle competenti strutture organizzative dell'Università.

2. L'Università si riserva la possibilità di applicare profili di navigazione personalizzati per gruppi di utenti o per settori, a seconda dell'attività professionale svolta. L'Università si riserva, altresì, la possibilità di applicare politiche di gestione della banda di trasmissione dati (traffic shaping) al fine di migliorare la fruibilità dei servizi legati alla ricerca, alla didattica ed ai servizi istituzionali in generale.

3. I dati relativi l'accesso alla rete universitaria e l'accesso ad Internet o al traffico telematico in generale (escluso il contenuto della trasmissione dati) sono memorizzati in appositi sistemi e periodicamente (ogni 6 mesi) cancellati in automatico dal sistema. Tali informazioni sono a disposizione dell'autorità giudiziaria la quale può richiedere la non cancellazione e la conservazione per un periodo più lungo. Tali informazioni sono utilizzate nella modalità aggregata (non riconducibile direttamente all'utente) per l'analisi del funzionamento della rete e per fini statistici.

4. L'accesso alla rete di Ateneo dovrà avvenire sempre, solo ed esclusivamente attraverso le modalità stabilite dagli Amministratori di rete che provvederanno a fornire le comunicazioni all'utente interessato.

5. In presenza di personal computer utilizzati da più utenti dovranno essere attivate procedure adeguate al fine identificare univocamente l'utilizzatore ed il lasso di tempo che ha lavorato al suddetto computer.

6. Non è, in ogni caso, consentito:

- fornire a soggetti non autorizzati l'accesso alla Rete di Ateneo o altri servizi di connettività di rete;
- navigare e/o registrarsi su siti non inerenti la propria attività istituzionale, di didattica e di ricerca;
- apportare modifiche alle impostazioni di accesso alla rete di Ateneo fornite dagli Amministratori di rete;

- utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete di Ateneo, sulla rete GARR e quelle ad essa collegate;
- creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
- scaricare, scambiare, condividere programmi e/o file in violazione del diritto d'autore;
- trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
- partecipare a forum o *chat line*, navigare e/o utilizzare software di social network se non per motivi relativi alla propria attività istituzionale, didattica e di ricerca;
- comunicare su siti di tipo *X-rated* (siti che contengono foto o filmati di carattere pornografico), Casinò virtuali, siti *Warez* (siti che diffondono codici per l'utilizzo di software senza acquistarne la licenza) e similari;
- porre in essere procedure atte ad eludere il sistema di sicurezza, eventuali filtri ed ogni altra attività con la quale si vuol nascondere la propria identità;
- collegare apparati di rete (Access Point WiFi, router, firewall, switch,... ) o attivare servizi (DHCP, NAT) se non preventivamente autorizzati dalla Ripartizione Servizi Informatici e Statistici e, in ogni caso, il loro utilizzo dovrà avvenire in conformità con il seguente regolamento;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy.

## **Art. 9**

### **Sviluppo e gestione Indirizzamento IP e domini**

1. La rete di Ateneo collega le strutture dell'Università alla Rete Italiana dell'Università e della Ricerca Scientifica gestita dal Consortium GARR. La Ripartizione Servizi Informatici e Statistici è responsabile dello spazio di indirizzamento IP e del dominio unipg.it assegnato all'Ateneo.

2. La gestione del dominio unipg.it e di tutti i sottodomini sono di competenza della Ripartizione Servizi Informatici e Statistici. La richiesta di un sottodominio del dominio unipg.it (xxxx.unipg.it) da parte di una struttura dell'Ateneo o da parte di un suo utente deve avvenire tramite un'apposita domanda alla Ripartizione medesima, a firma del Responsabile della struttura ed eventualmente dell'utente richiedente, nella quale risulti il nome del responsabile del sottodominio e l'accettazione del presente regolamento.

3. La progettazione, lo sviluppo e la gestione della rete d'Ateneo, i server che erogano servizi centralizzati di rete (DNS, AAA Server, Firewall, etc...), gli apparati attivi, i collegamenti metropolitani rientrano tra i compiti della Ripartizione Servizi Informatici e Statistici.

4. E' possibile registrare nuovi domini sotto il ccTLD "IT" e sotto il TLD "EU" solo ed esclusivamente attraverso la Ripartizione Servizi Informatici e Statistici per conto del GARR. Non è consentita la registrazione di domini con altri Mantainer e sotto altri TLD (Top Level Domain) o associare indirizzi universitari a nomi a dominio diversi da quelli autorizzati.

## **Art. 10**

### **Posta elettronica**

1. A mente dell'art. 47 del d.lgs 7 marzo 2005, n. 82 (*Codice dell'Amministrazione digitale*) e secondo quanto ribadito anche dalla circolare n. 1/2010/DDI, l'Amministrazione è tenuta a utilizzare la posta elettronica anche per le comunicazioni con i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

La casella di posta elettronica assegnata è, pertanto, uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento dell'attività lavorativa, di didattica e di ricerca.

2. Sono utenti assegnatari della casella di posta elettronica i dipendenti assunti a tempo indeterminato, determinato e i collaboratori che, per le funzioni svolte, sono dotati di personal computer.

3. L'utilizzo della casella e-mail assegnata in modalità istituzionale è consentito:

- a tutto il personale, a tempo determinato e indeterminato dell'Università, mediante una casella di posta istituzionale;
- a tutti gli studenti iscritti ai corsi di laurea, dottorandi, specializzandi, mediante la casella di posta assegnata;
- agli assegnisti di ricerca e personale a contratto per la realizzazione di specifici progetti;
- alle strutture dell'Ateneo;
- ad ogni utente espressamente autorizzato in base all'attività svolta all'interno dell'Università.

## **Art. 11**

### **Gestione e utilizzo delle caselle di posta elettronica**

1. Gli utenti, nell'utilizzare la posta elettronica, devono attenersi alle seguenti prescrizioni:

- non è consentito l'utilizzo delle caselle di posta elettronica dell'Università per attività personali non attinenti le proprie mansioni e la propria attività istituzionale;

- in caso di assenza prolungata o improvvisa, il singolo dipendente deve adoperarsi per delegare un altro dipendente a leggere i propri messaggi e inoltrare quelli ritenuti importanti per lo svolgimento dell'attività lavorativa. Qualora tale accorgimento non venga posto in essere dal dipendente ovvero questi si trovi nell'impossibilità di provvedere a quanto previsto, l'Amministrazione, su richiesta della struttura interessata, si riserva di procedere all'accesso, a tutela del buon andamento e dell'efficienza dell'attività istituzionale;

- le caselle di posta elettronica private, il cui accesso è ammesso limitatamente attraverso il sistema web, non possono essere utilizzate per l'attività istituzionale;

- l'uso della posta elettronica non è comunque consentito per partecipare a forum e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio;

- è fatto divieto di inviare messaggi con contenuti che non rispettino la normativa sulla proprietà intellettuale.

2. Le suddette regole comportamentali dovranno essere rispettate anche per la gestione e l'utilizzo delle *mailing list* delle strutture d'Ateneo, ove presenti.

## **CAPO IV**

### **CONTROLLI**

## **Art. 12**

### **Monitoraggio e controlli**

1. In caso di riscontrate e/o segnalate anomalie, l'Università si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici, compresa la verifica del traffico anomalo generato.

2. Per esigenze organizzative, produttive e di sicurezza l'Università può effettuare, altresì, controlli di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti.

3. Qualora, durante i controlli di cui ai punti precedenti, vengano rilevati utilizzi degli strumenti informatici in modalità difformi a quanto previsto dal presente documento o dalle normative nazionali, statutarie e regolamentari vigenti, l'Amministrazione adotterà le opportune, conseguenti determinazioni, in

maniera proporzionata alla criticità rilevata e comunque nel rispetto del principio di non eccedenza e dei limiti previsti nel nostro ordinamento.

### **Art. 13**

#### **Profili di Responsabilità**

1. Ferme restando le prescrizioni normative previste al d.L. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*) nonché al d.lgs. 7 marzo 2005, n. 82 (*Codice dell'Amministrazione digitale*), il dipendente è responsabile disciplinarmente, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi, dei programmi e del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche ai sensi della normativa regolamentare e statutaria di questa Università.
2. L'indebito utilizzo della connessione a Internet e della casella e-mail da parte del dipendente configura profili di responsabilità a carico del medesimo per il danno erariale cagionato all'Amministrazione, consistente nel mancato e/o scorretto svolgimento della prestazione lavorativa durante le ore di connessione.
3. Sono altresì responsabili del mancato rispetto delle prescrizioni contenute nel presente regolamento tutti i soggetti preposti al controllo, già individuati in ragione delle proprie funzioni apicali e organizzative ai sensi del D.R. 1077 del 01 giugno 2004 e successivi atti e provvedimenti.

### **Art. 14**

#### **Norma di rinvio**

1. Per tutto quanto non disciplinato al presente regolamento è fatto esplicito rinvio alle normative, anche statutarie e regolamentari, previste in materia.