UNIVERSITÀ DEGLI STUDI «G. D'ANNUNZIO»
CHIETI - PESCARA

REGOLAMENTO DI UTILIZZO DELLA RETE INTERNET E DELLA POSTA ELETTRONICA

(emanato con D.R. n. 1158 del 9 settembre 2014)

INDICE

Art. 1 - Oggetto e ambito di applicazione

1. Il presente regolamento disciplina le modalità di accesso e di uso di Internet e dei servizi che, tramite la rete, è possibile ricevere o offrire all'interno o all'esterno dell'Università degli Studi "G. d'Annunzio" (di seguito "Ateneo"), nel rispetto del Codice in materia di protezione dei dati personali (D. Lgs. 30 giugno 2003, n. 196), delle Linee guida del Garante per la protezione dei dati personali adottate con delibera n. 13 del 1/3/2007 (G.U. n. 58 del 10/3/2007) e del regolamento di Ateneo sul trattamento dei dati personali.

2. L'Ateneo si avvale delle risorse informatiche e telematiche per lo svolgimento ottimale delle sue funzioni istituzionali e per la gestione amministrativa. La rete di Ateneo collega permanentemente le diverse sedi in cui si articola l'Ateneo. Essa è interconnessa alla rete Garr e, tramite quest'ultima, alla rete Internet. L'uso delle risorse e dei servizi Internet tramite la rete di Ateneo è pertanto subordinato anche al rispetto delle norme dettate dagli organi di governo del Garr in ordine all'accesso e all'utilizzo della stessa rete Garr.

3. Le norme relative all'uso della rete Garr emanate ed emanande dai responsabili della rete Garr fanno parte integrante del presente regolamento (allegato A).

4. Per quanto non espressamente previsto nel presente regolamento, si fa rinvio alla normativa vigente in materia.

Art. 2 - Definizioni

1. Nel presente regolamento i termini di seguito elencati hanno il significato ai medesimi associato:
Struttura: Articolazione istituzionale dell'Ateneo: Scuole, Dipartimenti, Centri, Aree/Settori e Servizi dell'Amministrazione Centrale;
Utenti: tutti coloro che hanno accesso alla rete di Ateneo ai sensi dell'art. 3 del presente regolamento;
Settore competente: personale tecnico appartenente all'Area Reti, sistemi, protocollo informatico e BDW – Settore Infrastrutture IT e TLC, addetto alla gestione della rete e delle infrastrutture informatiche e telematiche (amministratori di sistema);
Rete di Ateneo: infrastruttura di collegamento informatico, telefonico e documentale dell'Ateneo. Comprende: cablaggio, apparati per la trasmissione dati e per la telefonia, applicativi per la gestione documentale e del traffico;
Posta elettronica: servizio di invio e ricezione di comunicazioni postali attraverso la rete telematica, sia indirizzata a singoli utenti che a gruppi;
Garr: Gruppo Armonizzazione Reti per la Ricerca creato nel 1988 che opera sotto la direzione del Ministero dell'Università e della Ricerca (MiUR);
Rete Garr: la rete italiana della ricerca, attualmente gestita dal Consortium GARR (Cnr, Enea, INFN, CRUI, Università, etc.);
Rete Internet: la rete geografica basata sul protocollo di comunicazione TCP/IP.

Art. 3 - Utenti della rete di Ateneo

1. Hanno diritto di accedere alla Rete di Ateneo:
a) i professori e i ricercatori dell'Ateneo;
b) il personale tecnico-amministrativo;

c) gli studenti;
d) i dottorandi di ricerca, gli specializzandi e gli assegnisti di ricerca;
e) i terzi (ad esempio: professori a contratto, visiting professors, etc.), su autorizzazione del responsabile della Struttura di riferimento e per il tempo limitato alla durata del rapporto intercorrente con l'Ateneo, nel rispetto del successivo art. 4.

2. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle risorse ed è consentito anche dall'esterno tramite Virtual Private Network (VPN) attraverso l'utilizzo delle credenziali (username e password) di rete, previa autorizzazione del Rettore e del Direttore Generale. Tale accesso dall'esterno è tecnicamente gestito dal Settore competente.

3. Tutti gli utenti che a qualsiasi titolo hanno accesso alla rete di Ateneo accettano senza riserve il presente regolamento. Per l'utilizzo del servizio VPN valgono le medesime regole riferite all'accesso alla rete dalle postazioni di lavoro dell'Ateneo.

Art. 4 - Stato dell'utenza

1. La condizione degli utenti in relazione all'utilizzo delle risorse può essere:
a) attiva: quando un utente ha accesso a tutti i servizi per i quali è autorizzato;
b) sospesa: quando un utente è privato temporaneamente dei diritti di utilizzazione delle risorse informatiche e telematiche a seguito di specifici provvedimenti amministrativi;
c) cessata: quando è cessato il rapporto intercorrente tra l'utente e l'Ateneo;
d) quiescenza: quando è cessato il rapporto intercorrente tra l'utente e l'Ateneo, ma l'utenza viene mantenuta attiva per un periodo di tempo, previa autorizzazione in cui viene specificata anche la durata del "prolungamento".

Art. 5 - Modalità di accesso alla rete

1. Gli utenti accedono alla rete di Ateneo ed alle sue risorse tramite il rilascio di credenziali costituite da un nome utente ed una password.

2. Gli utenti di cui all'art. 3, comma 1, lett. a), b), c) e d) ottengono le credenziali automaticamente, tramite il Settore competente (matricola stipendiale/matricola d'iscrizione + password).

3. Agli utenti di cui all'art. 3, comma 1, lett. e) le credenziali sono assegnate dal Settore competente, su richiesta dell'interessato, previa autorizzazione (matricola ad hoc + password).

4. Le credenziali di accesso (nome utente e password) sono strettamente personali. Al primo accesso è obbligatorio per gli utenti modificare la password assegnata, in modo che la stessa sia di loro esclusiva conoscenza.

5. Gli utenti sono tenuti a conservare le proprie credenziali, avendo cura che esse non siano utilizzate da terzi. Ogni attività non regolare e/o commessa da terzi utilizzando credenziali altrui è imputata al titolare delle credenziali stesse.

6. L'accesso alla rete in modalità wireless è concesso agli utenti sulla base delle credenziali rilasciate ai sensi dei precedenti commi.

Art. 6 - Utilizzo computer, periferiche, materiale di consumo

1. Sui computer di proprietà dell'Ateneo non è consentito:

a) installare programmi non inerenti l'attività lavorativa e/o privi di licenze d'uso legali;
b) modificare le configurazioni relative all'accesso alla rete di Ateneo comunicate al momento della installazione (es. numero IP);
c) installare modem e altri apparati per l'accesso da/all'esterno se non preventivamente autorizzati;
d) copiare su dispositivi esterni personali dati la cui titolarità è dell'Ateneo;

2. L'utilizzo delle stampanti e dei materiali di consumo (carta, toner, CD-Rom, DVD) è riservato alla preparazione di materiale didattico, scientifico, amministrativo o comunque inerente l'attività istituzionale dell'Ateneo.

Art. 7 - Rete Internet

1. L'utilizzo di Internet è consentito agli utenti autorizzati ai sensi degli artt. 3 e 5 del presente regolamento, su tutti i personal computer e altri dispositivi connessi in qualsiasi modalità prevista alla rete.

2. È vietato usare la rete:

a) in modo difforme da quanto previsto dalle norme di legge e regolamentari;
b) per navigare e/o registrarsi su siti per scopi incompatibili con le finalità e con l'attività istituzionale dell'Ateneo;
c) per scaricare programmi e/o file coperti da diritto d'autore se non espressamente autorizzati e che comunque non siano in relazione con l'attività istituzionale;
d) per partecipare a forum, utilizzare programmi di chat e messaggistica per motivi non inerenti l'attività istituzionale;
e) per tentare accessi fraudolenti a dati, programmi e sistemi interni o esterni all'Ateneo;
f) per utilizzare credenziali di accesso diverse da quelle di cui si è assegnatari;
g) per commettere attività che violino la riservatezza di altri utenti o di terzi;
h) per attività che influenzino negativamente la regolare operatività della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti ai sensi delle norme Garr;
i) per attività che distraggano risorse (persone, capacità, elaboratori) in misura anomala, ai sensi delle norme Garr;
l) per la connessione di apparati di rete (es. hub, switch, router, access point wireless, firewall, etc.) non autorizzati dal Settore competente;
m) per effettuare nelle Strutture i cablaggi per il collegamento alla Rete di Ateneo senza l'autorizzazione del Settore competente.

3. È inoltre vietato usare l'anonimato o servirsi di risorse che consentono di restare anonimi.

Art. 8 - Posta elettronica, account e indirizzi

1. L'account di posta elettronica (username, password ed indirizzo di posta) è fornito gratuitamente, insieme ad un limitato spazio disco, come di seguito descritto:
- **Utenti** di cui all'art. 3, comma 1, lett. a), b), d), e) mediante una casella di posta istituzionale nella forma nome.cognome@unich.it oppure, nei casi di omonimia, nome.cognome1@unich.it
- **Studenti** mediante una casella di posta istituzionale nella forma nome.cognome@studenti.unich.it oppure, nei casi di omonimia, nome.cognome1@studenti.unich.it

- **Cariche accademiche, strutture ed organizzazioni interne** mediante una casella di posta istituzionale nelle forme: carica@unich.it, struttura@unich.it

2. L'attivazione dell'account avviene a cura del Settore competente, previa verifica delle condizioni di cui all'art. 3 del presente regolamento.

3. Nell'esercizio del servizio di posta, il personale tecnico competente non può esercitare visura, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti ed inviati dagli utenti, fatte salve le normali operazioni di intercettazione da parte di appositi filtri automatici di virus o spam contenuti nei messaggi stessi e ad eccezione dei casi in cui ciò si renda necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o a disposizioni delle Autorità di Pubblica Sicurezza.

4. L'Ateneo adotta procedure per l'effettuazione e la conservazione di copie di sicurezza (backup) della posta elettronica ai sensi dell'art. 34 del Codice in materia di protezione dei dati personali.

Art. 9 - Posta elettronica certificata

1. La Posta Elettronica Certificata (PEC) di Ateneo è un sistema di posta elettronica nel quale è fornita al mittente l'attestazione elettronica dell'invio e della consegna del messaggio, garantendo una ricevuta di ritorno conforme all'attuale normativa e pertanto avente valore legale.

2. Il servizio di PEC è gestito dal Settore competente affidandosi ad un "Gestore del servizio di posta elettronica certificata" riconosciuto ed è obbligatorio, in base al Codice di Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e s.m.i.), per tutte le A.O.O. (Aree Organizzative Omogenee) di Ateneo e in tutti i casi in cui sia previsto dalla normativa vigente in materia.

3. Il formato della casella assegnata è aoo@pec.unich.it; essa deve essere usata per soli fini istituzionali per l'invio di messaggi di posta ad altre caselle di posta PEC.

Art. 10 - Utilizzo della posta elettronica

1. Nell'utilizzo del servizio di posta elettronica dell'Ateneo, ogni utente è tenuto ad attenersi alle seguenti regole:
- i messaggi contenuti nella casella di posta elettronica vanno letti con frequenza (si consiglia almeno una volta per ogni giorno lavorativo);
- la posta che non si intende conservare sul server deve essere eliminata al fine di non occupare inutilmente lo spazio disco sul server stesso;
- in caso di assenza prolungata o improvvisa il singolo dipendente deve essere messo in condizioni di delegare un altro dipendente a leggere i propri messaggi e inoltrare quelli ritenuti importanti per lo svolgimento dell'attività lavorativa;
- la casella di posta di ogni singola Struttura può essere utilizzata da più dipendenti secondo quanto stabilito dal Responsabile della Struttura stessa.

2. È vietato l'utilizzo della posta elettronica per fini non coincidenti con quelli istituzionali. È vietato altresì l'uso di caselle di posta elettronica personali (non istituzionali) per l'attività istituzionale.

3. È vietato l'utilizzo della posta elettronica per partecipare a forum e/o dibattiti se non per motivi istituzionali; per diffondere notizie non veritiere o quanto altro abbia contenuto offensivo e discriminatorio; per inviare messaggi con contenuti che violino la normativa sulla proprietà intellettuale; per inviare lettere a catena ovvero messaggi ripetuti; per diffondere messaggi di provenienza dubbia.

4. Il Settore competente ha facoltà di richiedere agli utenti, in qualunque momento, la diminuzione dello spazio disco occupato in relazione alle esigenze generali connesse al servizio.

5. Non è previsto che un dipendente in servizio possa richiedere la disattivazione della propria casella di posta elettronica.

Art. 11 - Liste di distribuzione

1. Sono costituite le mailing list di tutto il personale dell'Ateneo suddivise per categoria e per funzioni. L'iscrizione alle mailing list è automatica una volta assegnata la casella di posta istituzionale e non è possibile effettuare la cancellazione.

2. Le mailing list sono adibite alla diffusione di informazioni di interesse generale, istituzionale e di servizio rivolte al personale.

3. Hanno diritto ad utilizzare le mailing list del personale:
- Il Rettore;
- I Prorettori e i Delegati del Rettore;
- Il Direttore Generale;
- Gli Organi Collegiali, previa apposita mozione;
- I Direttori di Dipartimento.

Art. 12 - Blog di Ateneo

1. Sulla rete di Ateneo è attivo un blog (blog.unich.it) che il personale autorizzato dal Rettore e dal Direttore Generale può utilizzare per diffondere notizie di interesse generale e accademico.

2. Gli utenti, autenticandosi con la propria matricola, hanno la possibilità di commentare tali notizie.

Art. 13 - Responsabilità individuali

1. I soggetti che utilizzano risorse informatiche all'interno della rete di Ateneo sono tenuti a:
- adottare, nell'ambito delle proprie attività, tutti i comportamenti e le misure di sicurezza indicate nel presente regolamento atti a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi che abbiano come mezzo o fine le risorse informatiche;
- mantenere un'adeguata riservatezza dei dati e in merito alle misure di sicurezza adottate e alle modalità di accesso ai servizi;
- adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni, per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti ed evitare che le attività svolte producano disturbo o danni ad altri utenti;
- utilizzare esclusivamente le risorse alla cui fruizione e per i fini per i quali sono autorizzati;

- evitare qualsiasi attività che possa produrre danni alle risorse informatiche dell'Ateneo o alla sua immagine o che risulti in contrasto con le norme del presente regolamento, con le indicazioni del Settore competente, con le norme di legge e regolamentari vigenti in materia;
- segnalare ogni accertata violazione delle norme del presente regolamento.

Art. 14 - Trattamento dei dati di accesso ai servizi Internet

1. Le attività di accesso ai servizi Internet ed in particolare l'utilizzo della posta elettronica sono registrati in forma elettronica. L'attività di registrazione avviene attraverso dei file di sistema, a cura del Settore competente, tramite procedure che ne garantiscono la custodia e la riservatezza. I file sono mantenuti per un periodo di 36 mesi.

2. I dati personali relativi all'utente e alle sue attività ed i contenuti che sono immessi e veicolati in rete non sono sottoposti a trattamento se non ai fini di legge o in relazione alle richieste dell'Autorità giudiziaria.

3. I dati relativi alle connessioni sono gestiti in maniera anonima e trattati esclusivamente in relazione alle attività di monitoraggio del servizio, alla sicurezza ed all'integrità dei sistemi.

Art. 15 - Sanzioni

1. La mancata osservanza del presente regolamento comporta la restrizione o la revoca delle autorizzazioni all'utilizzo dei servizi, comminate dal Rettore su indicazione del Settore competente, a seguito di valutazione della gravità delle violazioni commesse e sentito l'utente. Sono fatte salve le più gravi sanzioni previste dalle norme vigenti.

2. Il Settore competente, nell'ambito della sua attività di gestione, adotta, nel rispetto dei limiti e delle procedure fissati dalla normativa vigente, misure di controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti Internet esterni, utilizzando opportuni mezzi tecnici e, qualora riscontri la violazione delle regole poste, rende informativa al Rettore e al Direttore Generale, ove ne ricorrano le circostanze, alle Autorità giudiziarie competenti per l'adozione degli eventuali provvedimenti di spettanza.

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

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

5. Si rende noto che, esclusivamente su precisa richiesta delle Autorità competenti, nel rispetto della normativa vigente in materia di privacy, è tecnicamente possibile risalire, in caso di violazioni delle regole, allo specifico utente utilizzatore. La consultazione dei suddetti file di tracciatura in maniera non aggregata è diritto esclusivo dell'Autorità giudiziaria, in conformità alle norme relative alla tutela della privacy.

6. Nelle ipotesi di uso difforme della rete dalle regolamentazioni Garr e, a seguito di segnalazione da parte dei gestori della rete medesima, il Settore competente è autorizzato alla immediata sospensione dell'accesso senza preavviso.

Art. 16 - Disposizioni finali

1. Al fine di assicurare politiche unitarie di gestione e sicurezza, le apparecchiature di rete di tipo switch e access point wireless, acquistate in autonomia dalle Strutture, per poter essere collegate alla rete di Ateneo, dovranno autorizzate ai sensi dell'art. 7, comma 1, lettera l) del presente regolamento, nonché essere rispondenti alle specifiche di quelle già in esercizio. Tali specifiche potranno essere richieste al Settore competente.

2. Le Strutture, nel realizzare e gestire in autonomia eventuali risorse non direttamente connesse alla rete di Ateneo (laboratori, reti di test, progetti specifici), non dovranno arrecare alcun disservizio, di natura tecnica o di sicurezza, ad altri utenti o alla rete di Ateneo.

3. Il Settore competente si riserva di emanare norme e procedure necessarie od utili per la corretta funzionalità e gestione tecnica della rete e dei suoi servizi.

4. Fanno parte integrante del presente regolamento: 1) le Norme Garr (Acceptable use policy Garr) di cui all'allegato A; 2) l'etica e le norme di buon uso dei servizi di rete (Netiquette) di cui all'allegato B.

ALLEGATO A

NORME GARR (ACCEPTABLE USE POLICY GARR)

1. La Rete Italiana dell'Università e della Ricerca Scientifica, denominata comunemente "la Rete GARR", si fonda su progetti di collaborazione scientifica ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MIUR. L'utilizzo della Rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale).
Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:
- fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonché permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
- 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 GARR e su 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;
- trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
- 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;
- svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonché dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete cui si fa accesso.
4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la

responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.

5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purché l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.

Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.

Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.

6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.

Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.

7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.

8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.

9. In caso di accertata inosservanza di queste norme di utilizzo della Rete, gli Organismi Direttivi del Consortium GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.

10. L'accesso alla Rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.

ALLEGATO B

NETIQUETTE

Etica e norme di buon uso dei servizi di rete

Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, ed in particolare fra i lettori dei servizi di "news" Usenet, si sono sviluppati nel corso del tempo una serie di "tradizioni" e di "principi di buon comportamento" (galateo) che vanno collettivamente sotto il nome di "netiquette".
Tenendo ben a mente che la entità che fornisce l'accesso ai servizi di rete (provider, istituzione pubblica, datore di lavoro, etc.) può regolamentare in modo ancora più preciso i doveri dei propri utente, riportiamo in questo documento un breve sunto dei principi fondamentali della "netiquette", a cui tutti sono tenuti ad adeguarsi.
1. Quando si arriva in un nuovo newsgroup o in una nuova lista di distribuzione via posta elettronica, è bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi in giro per il mondo: in tale modo ci si rende conto dell'argomento e del metodo con cui lo si tratta in tale comunità.
2. Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema.
3. Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione.
4. Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale.
5. Non condurre "guerre di opinione" sulla rete a colpi di messaggi e contromessaggi: se ci sono diatribe personali, è meglio risolverle via posta elettronica in corrispondenza privata tra gli interessati.
6. Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica.
7. Non pubblicare messaggi stupidi o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione. Leggere sempre le FAQ (Frequently Asked Questions) relative all'argomento trattato prima di inviare nuove domande.
8. Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito.
9. Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.
Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso:
A) La rete è utilizzata come strumento di lavoro da molti degli utenti. Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.
B) Qualunque attività che appesantisca il traffico sulla rete, quale per esempio il trasferimento di archivi voluminosi, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in orari diversi da quelli di massima operatività (per esempio di notte), tenendo presenti le eventuali differenze di fuso orario.
C) Vi sono sulla rete una serie di siti server (file server) che contengono in copia aggiornata documentazione, software ed altri oggetti disponibili sulla rete. Informatevi preventivamente su

quale sia il nodo server più accessibile per voi. Se un file è disponibile su di esso o localmente, non vi è alcuna ragione per prenderlo dalla rete, impegnando inutilmente la linea e impiegando un tempo sicuramente maggiore per il trasferimento.
D) Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o redistribuirlo in qualunque modo e sotto qualunque forma.
E) Comportamenti palesemente scorretti da parte di un utente, quali:
- violare la sicurezza di archivi e computers della rete;
- violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
- compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente; costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge.