IMT SCUOLA ALTI STUDI LUCCA

REGOLAMENTO PER L'USO DELLA RETE E DELLA POSTA ELETTRONICA

Titolo 1 Caratteri generali

Articolo 1 - Riferimenti

1. Il presente regolamento è un atto dovuto, previsto dal provvedimento del Garante per la Privacy pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007. Tale provvedimento, prescrive ai datori di lavoro pubblici e privati di stilare un disciplinare relativo all'utilizzo di internet e della posta elettronica nei posti di lavoro, indicando in che misura e con quali modalità siano effettuati eventuali controlli.
2. Il regolamento è stato stilato tenendo presenti i riferimenti alla policy di utilizzo della rete da parte del GARR (la rete della ricerca che consente la connettività verso Internet), il contratto Google Apps for Education, le norme sulla privacy di Google e la Netiquette.

Articolo 2 - Oggetto e ambito di applicazione

1. Il presente regolamento stabilisce le condizioni di utilizzo della posta elettronica, della connettività di rete e dei sistemi informativi forniti dalla Scuola, a supporto della didattica, della ricerca, dell'amministrazione e di altre attività correlate ai fini istituzionali della Scuola. Il servizio offerto all'Utente è subordinato alla presa visione del presente regolamento in tutte le sue parti e all'accettazione integrale e senza riserve delle condizioni previste..
2. L'utente si indentifica alla posta elettronica, alla rete e ai sistemi informativi mediante credenziali distinte. Le credenziali sono coppie di nome utente e password, l'accesso alla posta elettronica può essere rinforzato mediante la verifica in due passaggi.
3. Tutti i servizi telematici della Scuola sono gestiti dall' ufficio Infrastrutture, servizi informatici e amministrazione digitale, che individua anche gli amministratori di sistema per i vari servizi.
4. Gli utenti che hanno diritto alle credenziali per l'accesso ai diversi servizi e la durata di tali credenziali sono definiti da apposito regolamento o provvedimento generale della Scuola.

Titolo 2 Posta elettronica

Articolo 3 - Google Apps for Education

1. Il servizio di posta elettronica della Scuola è parte dei servizi denominati Google Apps for Education ed è fornito da Google Inc. («Google»), con sede a 1600 Amphitheatre Parkway, Mountain View, CA 94043, Stati Uniti, secondo il termini del Contratto Google Apps for Education.
2. Le credenziali per l'accesso ai servizi di posta elettronica fornite dalla Scuola permettono l'accesso alla propria casella di posta elettronica istituzionale.
3. Chiunque utilizzi una casella di posta elettronica della Scuola è edotto del fatto

che gli amministratori di IMT sono dotati da Googl dei mezzi tecnici per accedere, monitorare, utilizzare idati degli account e accetta:

   a. che i propri dati possono essere memorizzati in *datacenter* fuori dai confini italiani;
   b. i termini di servizio e le norme sulla privacy di Google che devono essere accettate la prima volta che si accede alla propria casella;
   c. i livelli di servizio definiti nel documento Contratto sul livello dei servizi (SLA) di Google Apps.

4. L'utilizzatore delle caselle di posta elettronica si impegna a:
    a. non generare o agevolare messaggi email collettivi non richiesti a scopo commerciale;
    b. non violare o incoraggiare la violazione di altrui diritti;
    c. non perseguire qualsivoglia finalità illecita, di intrusione, di violazione, di diffamazione o di frode;
    d. non diffondere intenzionalmente virus, worm, Trojan horse, file danneggiati, hoax o qualsivoglia materiale di natura distruttiva o ingannevole;
    e. non inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
    f. adoperarsi attivamente per salvaguardare la riservatezza della sua password e a segnalare qualunque situazione che possa inficiarla
    g. rispettare quanto previsto in materia dall'art. 11 del Codice di Comportamento di IMT

    L'elenco riportato e da intendersi non esaustivo.

Articolo 4 - Caselle di posta elettronica istituzionale

1. Ad ogni utente avente diritto viene creata una credenziale per l'accesso alla casella di posta elettronica istituzionale, il cui nome utente è nella forma nome.cognome@imtlucca.it e un *alias* corto, primaletteradelnome.cognome@imtlucca.it (alcuni account storici potrebbero essere impostati diversamente e cioè la credenziale principale nella forma primaletteradelnome.cognome@imtlucca.it e un alias nella forma nome.cognome@imtlucca.it).
2. Gli *alumni* della Scuola mantengono la loro casella di posta elettronica attraverso gli alias ma il nome utente principale viene trasformato nella forma nome.cognome@alumni.imtlucca.it.
3. L'attivazione e la disattivazione delle caselle di posta elettronica istituzionale è a cura degli amministratori di sistema. Per giustificati motivi è possibile richiedere l'inoltro della propria casella di posta elettronica verso una casella personale anche dopo la disattivazione o la scadenza dei termini.
4. Non è consentito l'accesso ad una casella di posta elettronica istituzionale da parte di più utenti contemporaneamente.
5. La Scuola equipara la posta elettronica tra utenti interni alla corrispondenza cartacea aperta, l'Utente si dichiara consapevole che la corrispondenza interna è visionabile dal datore di lavoro.

Articolo 5 - Accesso senza assenso

1. La Scuola non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. La Scuola può consentire o disporrel'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, nei seguenti casi:
    a. su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
    b. previo preavviso all'utente, per gravi e comprovati motivi che facciano credere che siano state violate le disposizioni di legge vigenti o le regole definite nel seguente regolamento;
    c. in situazioni critiche e di emergenza.
2. La Scuola può permettere il reset della password utente qualora si ritenga ragionevolmente che le credenziali siano state sottratte all'insaputa dell'utente.

Articolo 6 - Sicurezza e riservatezza

1. I messaggi di posta elettronica possono essere soggetti ad un esame automatico da parte sia di Google (vedere le norme sulla privacy di Google) che di software anti-virus e anti-spam.
2. La Scuola si pone come obiettivo fondamentale che la posta elettronica sia sicura ed affidabile anche interagendo tempestivamente con il supporto tecnico di Google. Va comunque ricordato che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui dispositivi personali. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili.

Articolo 7 - Liste di distribuzione

1. Con provvedimento della Scuolasono definite le liste di distribuzione di tutto il personale della Scuola suddivise per categoria e funzioni. L'iscrizione alle liste di distribuzione è automatica una volta assegnata la casella di posta istituzionale.
2. Le liste di distribuzione sono adibite alla diffusione d'informazioni di interesse generale e comunque di servizio rivolte ai membri.

Articolo 8 - Liste di distribuzione, messaggi indesiderati

1. I messaggi classificati automaticamente (dal filtro antispam e dal software antivirus) come indesiderati e indirizzati alle liste di distribuzione vengono inseriti in una coda di moderazione nell'attesa di essere eliminati del tutto.
2. Gli utenti devono tener presente che, nell'assolvimento dei propri compiti, gli amministratori di sistema potrebbero visualizzare un messaggio indirizzato ad una lista di distribuzione erroneamente marcato come spam. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.
3. Per limitare il numero di messaggi indesiderati gli amministratori di sistema scelgono, a seconda dell'utilizzo della lista di distribuzione, di restringere l'elenco dei possibili mittenti utilizzando le diverse opzioni a disposizione, per esempio è possibile dare il diritto di inviare messaggi di posta ad una determinata lista di distribuzione solo a coloro che ne fanno parte.

Articolo 9 - Indirizzi di posta elettronica generali

1. Nella pagina della trasparenza, nella sezione relativa all'articolazione degli uffici sono pubblicati gli indirizzi di posta elettronica generali gestiti dagli uffici.
2. È possibile che ad un determinato ufficio vengano associati più indirizzi di posta elettronica generali per meglio permettere lo smistamento della posta elettronica suddivisa per attività dell'ufficio.
3. Gli indirizzi di posta elettronica generali sono gestiti mediante la tecnica delle liste di distribuzione e sono a tutti gli effetti da considerarsi liste di distribuzione. A differenza delle liste di distribuzione ordinarie agli indirizzi di posta elettronica generale è consentito inviare messaggi di posta elettronica con mittente l'indirizzo di posta elettronica della lista di distribuzione. Quando viene inviato un messaggio di posta elettronica con le suddette modalità, una copia del messaggio viene recapitata automaticamente a tutti i membri che fanno parte della lista di distribuzione che definisce l'indirizzo di posta elettronica generale. Si stabilisce in questo modo la collaborazione dell'attività tra tutti gli iscritti alla lista di distribuzione.
4. Grazie al meccanismo delle liste di distribuzione è possibile, senza operare direttamente sulle singole postazioni di lavoro, abilitare o disabilitare l'accesso agli indirizzi di posta elettronica

generale agendo direttamente sul pannello di amministrazione del server. Gli amministratori di sistema possono infatti, ad ogni modifica dell'articolazione degli uffici o delle attività, operare modifiche immediate ai membri delle liste di distribuzione (e quindi degli indirizzi di posta elettronica generali) dalla *consolle* di amministrazione.

5. Eccezionalmente, se ad un indirizzo di posta elettronica generale ha accessouna singola persona, l'indirizzo può essere gestito mediante una casella di posta elettronica tradizionale, la cui responsabilità è della persona che vi accede. In questi casi non sono previsti accessi alla casella di posta elettronica generale in caso di assenza dal lavoro del titolare.

Articolo 10 - Indirizzo di posta elettronica certificata (PEC)

1. L'indirizzo di posta elettronica certificata della Scuola, imtlucca@postecert.it è assegnato all' ufficio che si occupa dello smistamento della posta certificata in arrivo. Lo smistamento e la protocollazione, avvengono mediante l'interfaccia del software di gestione del protocollo informatico.

Titolo 3 Accesso alla rete d'Istituto

Articolo 11 - Accesso alla Rete

1. L'accesso a Internet della Scuola è fornito dal GARR attraverso la rete della ricerca.
2. Ogni utilizzatore del servizio Internet accetta le regole di accesso alla rete riportare nel documento denominato GARR Acceptable Use Policy – AUP.
3. Non sono ammesse sulla Rete le seguenti attività:
    a. fornire a soggetti non autorizzati all'accesso alla Rete 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 (third party routing);
    b. diffondere virus, hoaxes o altri programmi in un modo che si danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete e su quelle ad essa collegate;
    c. creare o trasmettere o immagazzinare (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;
    d. trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
    e. 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;
    f. svolgere sulla Rete attività che influenzino negativamente la regolare attività operativa della rete o ne restringano l'utilizzabilità e le prestazioni per gli altri utenti;
    g. svolgere sulla Rete ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale.
4. Ogni utilizzatore del servizio Internet si impegna, altresì, a rispettare, regolamenti e consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di rete cui si fa accesso.

Articolo 12 - Accesso alla Rete: credenziali

1. Gli utenti accedono alla rete istituzionale mediante le proprie credenziali di rete. Le credenziali di rete permettono l'autenticazione alla rete interna. Le stesse credenziali permettono liberamente di autenticarsi alla coda di stampa di tutte le stampanti abilitate. Durante la prima configurazione lo staff dell'Ufficio Infrastrutture, servizi informatici e amministrazione digitale controlla che il sistema operativo del dispositivo o dei dispositivi utente sia adeguatamente aggiornato e che sia eventualmente disponibile un antivirus anche esso aggiornato.
2. Per motivi di sicurezza è possibile accedere alla rete con qualunque dispositivo personale solo se munito di un sistema operativo aggiornato e se la data di messa in produzione del sistema operativo non abbia superato il decimo anno di vita.
3. Agli ospiti è consentito accedere alla rete mediante le loro credenziali *Eduroam* se disponibili.
4. Gli ospiti che ne fanno richiesta accedono alla rete denominata IMT-Guest con credenziali apposite facilmente impostabili mediante un qualunque browser web. Per motivi di sicurezza la rete IMT-Guest è separata dalla rete interna poiché sui dispositivi degli ospiti non viene effettuato alcun controllo di sicurezza. Si connettono alla rete IMT-Guest anche tutti i dispositivi utente che non superano i controlli di sicurezza per accedere alla rete di cui ai commi 1 e 2 presente articolo.
5. Sui dispositivi degli ospiti, specialmente quelli particolarmente datati e/o senza un programma antivirus aggiornato non viene garantito alcun tipo di supporto tecnico per la connessione.
6. Il nome utente delle credenziali è specificato nella forma nome.cognome seguito ove richiesto da una chiocciolina e dal dominio di autenticazione (per es. nome.cognome@imtlucca.it), in caso di omonimia il nome utente segue la numerazione successiva (per es. nome.cognome1).

Articolo 13 - Accesso alla Rete registrazione dei log di traffico

1. Gli estremi del traffico generato nella rete interna vengono memorizzati in forma di *log* anonimi su apposito dispositivo e i log conservati per un periodo di 200 (duecento) giorni.
2. I dettagli relativi alle autenticazioni alla rete sono memorizzati sui server che si occupano delle autenticazioni e conservati per un periodo 200 (duecento) giorni.
3. I log di sicurezza degli apparati di rete sono disponibili su un server dedicato.
4. L'Utente deve tenere presente che alcun modo viene effettuata registrazione alcuna del contenuto delle comunicazioni e che tutti i log sono accessibili solo dagli amministratori di sistema.

Articolo 14 - Accesso alla Rete filtri automatici

1. Sono attivi sulla rete dei filtri di riconoscimento automatico che impediscono l'esecuzione di alcuni software *Peer to Peer* eccessivamente dannosi dal punto di vista dell'utilizzo di banda e il cui utilizzo generale è il download di materiale protetto dal diritto d'autore.
2. Sono attivi sulla rete dei filtri di riconoscimento automatico che impediscono l'esecuzione di alcuni software utilizzati per aggirare i filtri di cui al comma precedente.
3. Per motivi di studio e di ricerca sono disponibili dei terminali per l'accesso alla rete senza blocco alcuno.

Titolo 4 Accesso al sistema informativo d'Istituto

Articolo 15 - Accesso al sistema informativo

1. Gli utenti accedono al sistema informativo della Scuola mediante le proprie credenziali di rete. L'accesso al sistema informativo è disponibile da qualunque postazione pubblica connessa ad Internet.
2. Le credenziali per l'accesso al sistema informativo di Istituto sono create automaticamente dal software di gestione contratti.
3. Le credenziali del Sistema Informativo sono utilizzate altresì per identificare l'utente ai servizi pubblicamente accessibili, come ad esempio la rete Eduroam, la federazione *IDEM* e il *proxy http* per la navigazione web.
4. Si applicano alla rete Eduroam disponibile nei locali della Scuola le stesse condizioni della rete degli ospiti.

Articolo 16 - Accesso al sistema informativo registrazione dei log di autenticazione

1. Le registrazioni delle autenticazioni ai servizi acceduti mediante le credenziali di ateneo sono disponibili sui server dedicati e mantenute per un periodo di 200 (duecento) giorni.
2. I log delle autenticazioni sono accessibili dagli amministratori di sistema.

Titolo 5 Disposizioni finali

Articolo 17 - Uso personale dei servizi telematici

1. È consentito l'utilizzo ragionevole delle proprie credenziali a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non:
   a. sia causa, diretta o indiretta di disservizi dei sistemi elaborativi;
   b. sia causa di oneri aggiuntivi per la Scuola;
   c. interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso la Scuola.

   L'utente è edotto del fatto che la Scuola considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica e il traffico di rete da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. La Scuola presuppone quindi che l'utente decida di utilizzare le proprie credenziali per scopi personali avendone preliminarmente e attentamente valutato l'opportunità.

Articolo 18 - Revoca del servizio

1. L'Utente riconosce e concorda che la Scuola possa revocargli le credenziali in caso di inattività per un periodo superiore a sei mesi. La revoca delle credenziali comporta la cancellazione dei dati.

Articolo 19 - Sanzioni

1. In caso di abuso o di violazione del presente regolamento, o di altri regolamenti della Scuola, a seconda della gravità del medesimo, e fatte salve le ulteriori conseguenze di natura penale, civile e amministrativa o disciplinare,possono essere comminate le seguenti sanzioni:

a. la limitazione, anche totale, dall'accesso alla rete da un minimo di una settimana a un massimo di sei mesi;
b. la revoca di tutte le credenziali con conseguente cancellazione dei dati.

2. Le sanzioni sono comminate dal Direttore Amministrativo su proposta dell'Ufficio Infrastrutture, servizi informatici e amministrazione digitale.
3. In caso abbia notizia di abuso e vi sia pericolo nel ritardo il Direttore Amministrativo può ordinare l'immediata cessazione dell'attività all'origine dell'abuso adottando le necessarie misure per impedire che l'abuso venga portato a ulteriori conseguenze.

Articolo 20 - Obblighi e limiti di responsabilità della Scuola

1. La Scuola si impegna ad utilizzare i dati forniti dall'Utente ai soli fini dell'erogazione e della gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo. La Scuola provvede alla predisposizione e alla diffusione dell'informativa, ai sensi dell'art. 13 d.lgs. n.196/2003 all'attivazione dei servizi.
2. La Scuola attua tutte le misure di sua competenza ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante non risponde in alcun modo ed è sollevato da ogni responsabilità ed obbligazione in relazione all'eventuale cancellazione, danneggiamento, mancato invio/ricezione o dell'omessa conservazione dei contenuti, derivanti da guasti e/o malfunzionamenti degli apparati di gestione e/o in generale del servizio stesso.

Articolo 21 - Modifiche al presente regolamento

1. Le modifiche al presente regolamento che derivano da nuove norme di legge e di regolamenti saranno adottate con apposito Decreto del Direttore Amministrativo e comunicate al Consiglio Direttivo nella prima seduta utile.