



Carta d'utilizzo del sistema d'informazione dell'École française de Rome
--

Sommario

Preambolo.....	3
Articolo I. Campo d'applicazione	3
Articolo II. Diritto d'accesso ai sistemi d'informazione	4
Articolo III. Protezione dei dati.....	4
Articolo IV. Condizioni d'uso dei sistemi d'informazione	4
Sezione IV.1 Uso professionale / privato.....	4
Articolo V. Principi di sicurezza.....	5
Sezione V.1 Norme di sicurezza applicabili.....	5
Sezione V.2 Doveri di segnalazione e d'informazione	5
Sezione V.3 Misure di controllo	5
Articolo VI. Comunicazione elettronica.....	6
Sezione VI.1 Messaggia elettronica	6
(a) Indirizzi di posta elettronica	6
(b) Contenuto dei messaggi di posta elettronica.....	6
(c) Invio e ricezione dei messaggi.....	6
Sezione VI.2 Internet	7
(a) Pubblicazione sui siti Internet e Intranet dell'Istituto.....	7
(b) Sicurezza	7
Sezione VI.3 Download	7
Articolo VII. Tracciabilità	7
Articolo VIII. Rispetto della proprietà intellettuale	7
Articolo IX. Rispetto della legislazione sui dati personali	7
Articolo X. Telelavoro.....	8
Articolo XI. Limitazioni d'uso.....	8
Articolo XII. Entrata in vigore della carta	8

Preambolo

La presente carta definisce le regole d'uso e di sicurezza che l'École française de Rome e l'utente s'impegnano a rispettare, e precisa i diritti e i doveri di ciascuno.

Il "sistema d'informazione" copre l'insieme delle risorse materiali e applicative, i programmi, i database e le reti di telecomunicazione locali, e quelle a cui è possibile accedere a distanza o a cascata a partire dalla rete dell'École française de Rome.

L'informatica nomade (palmari, computer portatili, telefoni portatili e così via) è anch'essa uno degli elementi costitutivi del sistema d'informazione.

Il buon funzionamento del sistema d'informazione presuppone il rispetto delle disposizioni legislative e normative, per quanto riguarda, in particolare, il rispetto delle regole miranti a garantire la sicurezza, l'efficienza del trattamento e della conservazione dei dati.

Il termine "utente" si riferisce a qualsivoglia individuo idoneo a possedere un account informatico o ad avere accesso alle risorse del sistema d'informazione, quale che sia il suo status.

Il termine "Istituto" designa l' "École française de Rome".

Il personale del servizio informatico incaricato dei sistemi d'informazione è tenuto al segreto professionale. Non può divulgare le informazioni di cui entra a conoscenza nell'ambito delle sue funzioni, nella misura in cui:

- le suddette informazioni siano protette dal segreto della corrispondenza o identificate come tali, e riguardanti la vita privata dell'utente;
- non compromettano il buon funzionamento del sistema d'informazione o la sua sicurezza;
- non contravvengano al rispetto della legislazione applicabile.

Obblighi dell'Istituto

L'Istituto informa l'utente dell'esistenza della presente carta.

L'Istituto, mediante il servizio informatico, adotta le misure necessarie a garantire la sicurezza del sistema d'informazione e la protezione degli utenti.

L'Istituto autorizza l'accesso degli utenti alle risorse del sistema d'informazione. Le risorse messe a disposizione sono destinate principalmente a un uso professionale; tuttavia, l'Istituto è tenuto a rispettare l'utilizzo residuale del sistema d'informazione a titolo privato.

Obblighi dell'utente

L'utente è responsabile, in ogni luogo e momento, dell'utilizzo del sistema d'informazione al quale ha accesso. Ha un obbligo di riservatezza riguardo alle informazioni e ai documenti prodotti o ai quali ha accesso. Tale obbligo implica il rispetto delle regole d'etica professionale e deontologiche¹.

L'utente s'impegna a rispettare scrupolosamente le regole indicate dal servizio informatico sull'utilizzo e sull'accesso, nonché le norme di sicurezza relative al sistema d'informazione.

L'utente è in ogni caso sottoposto al rispetto degli obblighi derivanti dal suo status o dal suo contratto.

L'utilizzo delle risorse messe a disposizione dell'utente deve essere ragionevole e corretto, allo scopo di evitare sovraccarichi o l'uso improprio a fini personali.

Articolo I. Campo d'applicazione

Le norme d'uso e di sicurezza incluse nella presente carta si applicano tanto all'Istituto quanto alla totalità degli utenti.

Gli utenti autorizzati ad accedere al sistema d'informazione comprendono:

- il personale dell'École française de Rome;

¹ In particolare, il segreto professionale in ambito medico.

- gli individui esterni all'Istituto, visitatori, invitati o prestatori², ricercatore in accoglienza, lettore della biblioteca, residente, invitato.

L'utilizzo specifico nell'ambito delle attività delle organizzazioni sindacali non è regolato dalla presente carta.

Le presenti norme si applicano a qualsivoglia individuo autorizzato all'utilizzo dei mezzi informatici dell'Istituto, inclusi i mezzi informatici condivisi o esternalizzati, e si estendono alle reti esterne accessibili mediante le reti dell'Istituto stesso.

Articolo II. Diritto d'accesso ai sistemi d'informazione

Il diritto d'accesso ai sistemi d'informazione è revocato se la qualifica dell'utente non ne giustifica più l'utilizzo, salvo nel caso di richiesta specifica, non oltre un mese dopo la scadenza del titolo che dà accesso all'account informatico.

Tale diritto può ancora essere revocato, a scopo cautelativo, qualora il comportamento dell'utente non fosse più compatibile con le norme indicate nella presente carta.

Articolo III. Protezione dei dati

L'utente è responsabile dei suoi dati professionali, o di quelli a cui ha accesso nell'ambito delle sue funzioni. In particolare, l'utente deve verificare il salvataggio dei suoi dati, vigilando sui diritti d'accesso che conferisce sugli stessi agli altri utenti.

L'utente deve garantire la protezione delle informazioni in generale. Per quanto riguarda i dati sensibili (per i quali è stata individuata una necessità diretta o indiretta di riservatezza), l'utente è tenuto, in particolare, a evitare di comunicarli o di trasmetterli senza protezione (crittografia) mediante supporti non adeguati (messaggeria, chiavetta usb, computer portatili, memorie esterne, e così via), o ad archivarli in un server esterno o accessibile al pubblico.

Articolo IV. Condizioni d'uso dei sistemi d'informazione

Sezione IV.1 Uso professionale/privato

L'uso dei sistemi d'informazione dell'Istituto ha per unico scopo la gestione delle attività di ricerca, di formazione, di documentazione, di valorizzazione e d'amministrazione. Se non autorizzati, i suddetti mezzi non possono essere impiegati in vista di un utilizzo o della realizzazione di progetti che esulino dalle missioni dell'Istituto o dalle missioni affidate agli utenti. Tuttavia, i suddetti mezzi possono essere utilizzati a supporto della comunicazione privata, alle condizioni sotto descritte.

L'utilizzo residuale del sistema d'informazione a titolo privato deve essere non lucrativo e ragionevole, sia nella frequenza, che per volume o durata. In ogni caso, gli eventuali costi aggiuntivi devono rimanere contenuti rispetto alle spese globali di funzionamento.

Il suddetto utilizzo non deve nuocere alla qualità del lavoro dell'utente, al tempo ad esso dedicato e al buon funzionamento del servizio.

Ogni informazione è considerata professionale, a esclusione dei dati esplicitamente indicati come appartenenti alla vita privata dell'utente, quali che siano i supporti (computer, chiave usb, telefono...) o i servizi (spazio di archiviazione, messaggeria) utilizzati.

In caso di necessità, l'istituto si riserva il diritto di consultare i dati presenti sui dispositivi (PC, dischi rigidi, chiavette USB, cartelle su strumenti condivisi...) messi a disposizione dell'utente (ad eccezione dei dati esplicitamente indicati come personali). Tale eventualità può verificarsi in particolare in caso di assenza prolungata (superiore a un mese) qualora la mancata consultazione della posta elettronica possa ostacolare il corretto funzionamento della struttura. In tal caso, l'utente ne sarà ufficialmente informato.

Pertanto, è dovere dell'utente procedere all'archiviazione dei suoi dati di carattere privato in uno spazio esplicitamente³ previsto a tale effetto, oppure indicandone la natura sulla risorsa utilizzata⁴. È compito dell'utente procedere con regolarità alla protezione e all'archiviazione dei dati di carattere privato.

L'utente è responsabile del suo spazio dati di natura privata. Nel momento in cui lasci definitivamente l'Istituto, l'utente è tenuto a eliminare lo spazio dati di natura privata, poiché l'Istituto non può essere tenuto responsabile della conservazione del suddetto spazio. In caso di decesso dell'utente, i suoi spazi privati saranno cancellati.

Le misure di conservazione dei dati professionali sono definite del servizio informatico dell'Istituto.

L'utilizzo a titolo privato dei sistemi d'informazione deve rispettare le norme vigenti.

² L'obbligo di rispetto della carta deve trovarsi espressamente indicato in ogni tipo di contratto.

³ Ad esempio, lo spazio potrebbe essere denominato « _privato_ »

⁴ Ad esempio, « _privato_nome_dell_oggetto_ », in cui per oggetto s'intende un messaggio, un file o qualsivoglia altra risorsa digitale.

Articolo V. Principi di sicurezza

Sezione V.1 Norme di sicurezza applicabili

Il servizio informatico applica i meccanismi di tutela adeguati sui sistemi d'informazione messi a disposizione degli utenti.

L'utente è informato del fatto che i codici d'accesso a lui attribuiti costituiscano una delle misure di sicurezza destinate a evitare qualsivoglia utilizzo malevolo o abusivo. Tale misura non conferisce agli strumenti informatici protetti un carattere personale.

L'utente non può registrare i codici d'accesso su supporti elettronici interni o esterni all'Istituto (computer, telefono, tablet...), anche se consentito da talune funzionalità del materiale informatico.

L'utente s'impegna a non trasmettere verso sistemi esterni i codici d'accesso.

I livelli di accesso autorizzati sono definiti in funzione della missione assegnata all'utente. La sicurezza dei sistemi d'informazione messi a disposizione dell'utente impone a quest'ultimo di:

- rispettare le norme di sicurezza, in particolare le regole relative alla gestione dei codici d'accesso, il cui utilizzo è posto sotto la responsabilità di ciascun utente;
- custodire in modo strettamente riservato i codici d'accesso, non rivelandoli a terzi;
- rispettare la gestione degli accessi, in particolare senza utilizzare, o tentare di acquisire i codici di accesso di altri utenti;
- bloccare la sessione al momento di lasciare la postazione di lavoro;

Inoltre la sicurezza delle risorse messe a disposizione dell'utente necessita di diverse precauzioni:

✓ da parte dell'Istituto:

- assicurarsi che le risorse sensibili non siano accessibili agli individui non abilitati;
- limitare l'accesso alle sole risorse per le quali l'utente sia espressamente abilitato.

✓ da parte dell'utente:

- non accedere, o tentare di accedere alle risorse del sistema d'informazione per le quali non abbia ricevuto un'autorizzazione esplicita;
- non accedere, o tentare di accedere alle risorse esterne o interne al sistema d'informazione dell'Istituto per le quali non abbia ricevuto un'autorizzazione esplicita;
- non consentire l'accesso (a materiali, risorse online, software...) ad altri utenti (interni o esterni) senza l'espressa autorizzazione del servizio informatico;
- non connettere direttamente alle reti locali materiali diversi da quelli autorizzati dal servizio informatico;
- non installare, scaricare o utilizzare sul materiale dell'Istituto programmi o pacchetti software diversi da quelli autorizzati dal servizio informatico;
- non utilizzare sulla rete wifi alcun computer personale non dotato di antivirus attivo, efficace e aggiornato; il suddetto computer non deve contenere malware (di analisi della rete, condivisione della banda...)
- non modificare o fare modificare da terzi il materiale e i programmi messi a disposizione dal servizio informatico;
- rispettare il diritto di proprietà intellettuale;
- conformarsi alle misure adottate dal servizio informatico per la lotta e la prevenzione degli attacchi (di virus, malware...);
- impegnarsi a non perturbare volontariamente il buon funzionamento delle risorse informatiche e delle reti, mediante manipolazioni anomale del materiale o dei programmi;
 - assicurarsi che il materiale messo a disposizione sia protetto contro il furto e i danni.

Sezione V.2 Doveri di segnalazione e d'informazione

L'utente segnalerà tempestivamente al servizio informatico i casi di malfunzionamento o qualsivoglia altra anomalia. Allo stesso modo, informerà il suo responsabile o i superiori qualora la possibilità di accesso a una risorsa non corrisponda all'abilitazione in suo possesso.

Sezione V.3 Misure di controllo

L'utente è informato che

- deve tempestivamente autorizzare e permettere al servizio informatico di effettuare interventi di manutenzione correttiva, curativa o evolutiva; il servizio informatico si riserva la possibilità di procedere a interventi (in caso di necessità, anche a distanza) sulle risorse messe a disposizione dell'utente;
- qualsiasi informazione che blocchi il sistema, o provochi una difficoltà tecnica nell'inoltro al destinatario della stessa, sarà isolata e, se necessario, soppressa;
- qualsiasi materiale corrotto o che costituisca una possibile minaccia al sistema d'informazione può essere immediatamente neutralizzato senza preavviso dal sistema d'informazione;
- il sistema d'informazione può essere oggetto di sorveglianza e controllo a fini statistici, di tracciabilità regolamentare o funzionale, di ottimizzazione, di sicurezza o d'individuazione di abusi, nel rispetto della legislazione applicabile.

Articolo VI. Comunicazione elettronica

Sezione VI.1 Messaggeria elettronica

L'utilizzo della messaggeria costituisce uno degli elementi essenziali d'ottimizzazione del lavoro, di reciprocità e di scambio d'informazione nell'ambito dell'Istituto.

(a) Indirizzi di posta elettronica

L'Istituto s'impegna a mettere a disposizione dell'utente, in caso quest'ultimo sia retribuito o legato da convenzione dell'Istituto stesso per un periodo superiore a due mesi, una casella di posta professionale nominativa, che consenta di inviare e ricevere messaggi di posta elettronica. La responsabilità dell'utilizzo dell'indirizzo nominativo ricade in seguito sull'utente.

L'utente utilizzerà il suddetto indirizzo di posta elettronica per comunicazioni riguardanti le azioni interne o esterne che contribuiscano all'adempimento delle missioni dell'Istituto.

L'utente s'impegna a non trasmettere verso sistemi esterni i codici d'accesso o l'utilizzo della sua casella postale.

La caratteristica nominativa dell'indirizzo di posta elettronica costituisce un semplice prolungamento dell'indirizzo di posta amministrativo/istituzionale: non priva in alcun modo la casella di posta del suo carattere professionale.

In caso di necessità, l'Istituto si riserva il diritto di consultare i messaggi ricevuti dall'utente (ad eccezione dei dati espressamente indicati come personali), il quale ne sarà in tal caso ufficialmente informato. Tale eventualità può verificarsi in particolare in caso di assenza prolungata (superiore a un mese), qualora la mancata consultazione della posta elettronica possa ostacolare il corretto funzionamento della struttura.

L'indirizzo di posta elettronica, che sia di funzione o di natura organizzativa, può essere creato sia per un utente o per un gruppo di utenti per le necessità dell'Istituto.

La gestione di indirizzi elettronici corrispondenti a liste di diffusione istituzionali, indicanti una categoria o un gruppo di "utenti", è di esclusiva responsabilità dell'Istituto. Le suddette liste non possono essere utilizzate senza autorizzazione.

(b) Contenuto dei messaggi di posta elettronici

I messaggi sono considerati di natura professionale a meno che non contengano indicazioni specifiche ed esplicite che ne rivelino il carattere privato⁵, o non siano archiviati in uno spazio dedicato ai messaggi privati.

Per garantire la continuità del buon funzionamento dei servizi, gli stessi possono essere soggetti a limitazioni, in particolare a soluzioni di trattamento dei messaggi indesiderati (spam, controllo dei virus...).

Sono proibiti i messaggi dai contenuti illeciti di qualsivoglia natura e che contravvengano, in particolare, alle disposizioni del Regolamento Generale sulla Protezione dei Dati (RGPD).

La trasmissione di dati sensibili⁶ è proibita a meno che non avvenga mediante un dispositivo specifico cifrato, autorizzato dal servizio informatico.

(c) Invio e ricezione dei messaggi

L'utente deve vigilare sulle informazioni ricevute (fake news, virus, frodi informatiche, catene di messaggi...).

L'utente deve verificare l'identità e l'esattezza degli indirizzi dei destinatari dei messaggi. È suo dovere vigilare affinché l'invio dei messaggi sia limitato ai soli destinatari pertinenti, in modo da evitare una diffusione massiva, l'inutile sovraccarico della messaggeria e, quindi, il deterioramento del servizio stesso.

⁵ Ad esempio, i messaggi il cui oggetto o soggetto comprendano il termine "privato".

⁶ Nell'ambito della protezione dei dati così come definita dal RGPD.

L'utente deve assicurarsi di rispettare il RGPD prima d'inviare i messaggi ai destinatari, in particolare per evitare che l'Istituto sia identificato come fonte di spam, il che penalizzerebbe pesantemente il servizio, causando il blocco della posta.

Section VI.2 Internet

Si ricorda che Internet è sottoposto alle norme giuridiche vigenti, e che il suo utilizzo e, per estensione, l'utilizzo dell'Intranet, costituisce uno degli elementi essenziali dell'ottimizzazione del lavoro, di reciprocità e di accessibilità dell'informazione nell'ambito dell'Istituto e al di fuori dello stesso.

Internet è uno strumento di lavoro che si presta a usi professionali (amministrativi, pedagogici o di ricerca). Si ricorda inoltre che se l'utilizzo residuale a carattere privato dello stesso, così come definito alla sezione III.1., può essere tollerato, si presume che le connessioni stabilite grazie allo strumento informatico messo a disposizione dall'Istituto abbiano un carattere professionale.

(a) Pubblicazione sui siti Internet e Intranet dell'Istituto

Qualsiasi forma di pubblicazione d'informazioni sui siti Internet o Intranet dell'Istituto deve essere convalidata dal responsabile del servizio o della pubblicazione specificatamente designato.

(b) Sicurezza

Per garantire la sicurezza del sistema d'informazione dell'Istituto il servizio informatico si riserva il diritto di filtrare o proibire l'accesso a taluni siti, di procedere al controllo preventivo o a posteriori dei siti visitati, d'intervenire sul sistema d'informazione dell'Istituto e di modificarlo.

Gli accessi sono autorizzati esclusivamente mediante i dispositivi di sicurezza adottati dal servizio informatico, il quale può indicare norme di sicurezza specifiche.

L'utente è informato dei rischi e dei limiti inerenti all'utilizzo di Internet mediante azioni di formazione con obbligo di frequenza o campagne di sensibilizzazione.

Sezione VI.3 Download

Ogni download o copia di file (in particolare suoni, immagini, programmi, corsi on-line...) su Internet o risorse locali deve essere effettuato nel rispetto dei diritti di proprietà intellettuale.

Il servizio informatico si riserva il diritto di limitare i download o la copia di taluni file di cui si accertasse la voluminosità o che presentassero rischi per la sicurezza dei sistemi d'informazione (virus, malware, spyware...).

Articolo VII. Tracciabilità

Il servizio informatico si riserva il diritto di adottare strumenti di tracciabilità e registro (*log*) su tutti i sistemi d'informazione.

Articolo VIII. Rispetto della proprietà intellettuale

L'Istituto ricorda che l'utilizzo delle risorse informatiche implica il rispetto dei corrispondenti diritti di proprietà intellettuale, così come quelli spettanti ai partners dell'Istituto e, più in generale, ai terzi titolari di tali diritti.

Di conseguenza, l'utente

- deve utilizzare i programmi secondo quanto contemplato dalle condizioni delle licenze sottoscritte;
- non deve riprodurre, copiare, diffondere, modificare o utilizzare programmi, database, pagine web, testi, immagini, fotografie o altre creazioni protette dal diritto d'autore o altro diritto privato, senza avere prima ottenuto l'autorizzazione scritta dei titolari dei diritti stessi, conformemente al modello fornito dall'Istituto.

Articolo IX. Rispetto della legislazione sui dati personali

L'utente ha l'obbligo di rispettare le disposizioni legali in materia di trattamento automatico dei dati di carattere personale, applicando il RGPD (protezione dei dati).

I dati di carattere personale sono informazioni atte a identificare direttamente o indirettamente e con qualsivoglia mezzo le persone fisiche alle quali si riferiscono.

La creazione di files comprendenti informazioni di questo tipo, e le richieste di trattamento ad esse relativo, anche qualora derivino dall'estrazione, incrocio o interconnessione di files già esistenti, è sottoposta a obblighi legali e deve essere stata oggetto di un'autorizzazione scritta dal delegato alla protezione dei dati (DPO) dell'Istituto.

Articolo X. Telelavoro

La pratica del telelavoro implica per l'utente la necessità di rispettare la totalità degli articoli della presente carta.

Il telelavoro è effettuato con il materiale informatico dell'Istituto, configurato dal servizio informatico e consegnato all'utente, oppure con il materiale informatico dell'utente stesso, debitamente convalidato dal servizio informatico, e se necessario, configurato da quest'ultimo, al fine di accedere a distanza al sistema d'informazione dell'Istituto permettendo così all'utente di svolgere le sue missioni.

La consegna all'utente del materiale informatico dell'Istituto dà luogo al conferimento di un buono di consegna firmato dall'utente.

Qualora l'utente utilizzi una connessione senza fili (wifi), la connessione deve utilizzare il massimo livello di cifratura e la rete non deve in nessun caso essere aperta.

Dietro richiesta del servizio informatico, il materiale messo a disposizione dall'Istituto deve essere immediatamente riconsegnato al servizio informatico.

Articolo XI. Limitazioni d'uso

In caso di non rispetto delle regole definite nella presente carta e delle modalità d'uso definite dal servizio informatico, l'uso del sistema d'informazione da parte dell'utente potrà essere soggetto, in via cautelativa, a limitazioni.

In caso di manomissione di un elemento interno o esterno al sistema d'informazione dell'Istituto, il servizio informatico ne potrà proibire l'uso.

Articolo XII. Entrata in vigore della carta

La carta informatica entrerà in vigore in data 17 settembre 2020.

Si trova in allegato al regolamento interno dell'Istituto e sarà aggiornata ogniqualvolta ciò sia necessario.

Aggiornamento il 12 giugno 2026.