ER.GO - AZIENDA REGIONALE PER IL DIRITTO AGLI STUDI SUPERIORI

Via Santa Maria Maggiore, 4, BOLOGNA

POLITICA AZIENDALE SULLA SICUREZZA INFORMATICA

Premessa generale

Il presente documento contiene le disposizioni, le misure organizzative e comportamentali che i dipendenti, i collaboratori a qualsiasi titolo dell'Azienda, gli studenti/utenti dei servizi aziendali sono chiamati ad osservare per contrastare i rischi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche messe a disposizione da ER.GO deve sempre ispirarsi al principio della diligenza e correttezza, con la presente ***Politica aziendale sulla sicurezza informatica*** s'intende contribuire alla massima diffusione della cultura della sicurezza in Azienda, evitando che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici/informativi e nel trattamento dei dati.

In particolare, il documento è suddiviso nelle seguenti tre parti:

1. *Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da ER.GO per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo*;

2. Norme comportamentali rivolte agli studenti delle residenze universitarie di ER.GO;

3. Regolamento per il corretto utilizzo dei *social media* di ER.GO.

Pubblicazione

Al presente documento - ed ai suoi futuri aggiornamenti - viene data massima diffusione attraverso la sua pubblicazione sul sito internet di ER.GO, www.er-go.it, sui canali social aziendali e sull'intranet aziendale.

§ § §

1. Regolamento sulle modalità di utilizzazione della strumentazione informatica messa a disposizione da ER.GO per lo svolgimento dell'attività lavorativa e sulle relative procedure di controllo.

Indice

Premessa

Il presente regolamento definisce le condizioni di utilizzo del Sistema informatico da parte dei collaboratori di ER.GO attraverso gli strumenti messi a disposizione dall'Azienda, per il pieno ed efficace svolgimento delle attività proprie dell'amministrazione e dei servizi ad esse correlati.

Tale Sistema informatico risponde ad usi ed obiettivi pubblici e aziendali e l'operatore che lo utilizza deve orientare il suo comportamento al perseguimento di tali scopi. L'utilizzo del Sistema è costantemente monitorato, nel rispetto della normativa sulla privacy e delle norme a tutela del lavoratore. Il regolamento prevede altresì un sistema sanzionatorio collegato all'uso improprio delle strumentazioni informatiche.

Tutti i beni che ER.GO mette a disposizione dei propri collaboratori per lo svolgimento dell'attività lavorativa devono essere utilizzati da parte di coloro che vi operano, a qualunque livello e con qualsiasi rapporto, in conformità ai principi espressi dal Codice di comportamento dei dipendenti pubblici D.P.R. n. 62 del 2013, nonché dal Codice di comportamento dei dipendenti di ER.GO adottato con deliberazione n. 25 del 17/04/2014.

1) Principi generali

L'utilizzo degli strumenti informatici forniti ai collaboratori aziendali deve avvenire in modo strettamente pertinente all'attività lavorativa, in maniera lecita, appropriata, efficiente e razionale, tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.

Deve altresì rispettare i principi etici e di correttezza e i doveri stabiliti nei sopracitati Codici di comportamento, nonché la privacy e la segretezza dei dati trattati secondo le normative vigenti.

In linea con quanto indicato dal Dipartimento della Funzione Pubblica (Direttiva n.02/09), il presente regolamento disciplina le modalità e finalità di utilizzo della strumentazione informatica, nonché le modalità di controllo di tale utilizzo, per garantire, nel rispetto della dignità e riservatezza delle persone in coerenza anche con la normativa vigente in materia di protezione dei dati personali (D.Lgs.n.196/2003) e con quanto prescritto dal Garante per la protezione dei dati personali con la delibera n.13 del 1°marzo 2007, la sicurezza dei dati e del sistema informatico aziendale.

2) Destinatari

Sono destinatari del presente Regolamento tutti i collaboratori di ER.GO con rapporto di lavoro subordinato (di qualsiasi tipologia) e coloro che svolgano, a qualsiasi titolo, attività per conto di ER.GO, accedendo al sistema informatico di quest'ultimo.

3) Modalità di utilizzo della strumentazione informatica

I destinatari di cui al punto 2) si impegnano ad utilizzare la strumentazione informatica nel rispetto dei principi di cui al precedente punto 1) e ad osservare le seguenti norme comportamentali:

3.1 Utilizzo di Internet

L'accesso alla rete Internet fornita dall'Azienda è consentito principalmente per scopi di studio e di ricerca e per l'accesso a dati ed informazioni concernenti l'attività aziendale; per motivi personali l'accesso è consentito soltanto in caso di necessità e comunque non in modo ripetuto o per periodi di tempo prolungati, evitando di:

a. accedere a siti e/o acquisire e/o diffondere contenuti informativi osceni, o lesivi dell'onorabilità individuale o collettiva, o altro materiale potenzialmente offensivo o diffamatorio. In particolare è vietata la ricezione, la trasmissione o il possesso di immagini pornografiche e/o pedo pornografiche.
b. partecipare ai *social network* (Facebook, MySpace, Twitter e simili), ai Blog, ai Forum di discussione, se ciò non è direttamente collegato alle attività lavorative rientranti nell'ambito della comunicazione esterna aziendale;
c. rimanere collegati per periodi di tempo prolungati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, in quanto ciò può appesantire il traffico della rete;
d. scaricare programmi, anche gratuiti, se ciò non è indispensabile allo svolgimento dell'attività lavorativa, segnalandolo preventivamente al proprio responsabile o all'assistenza informatica;
e. accedere a servizi con finalità ludiche o a chat line;

f. accedere a siti per la condivisione e lo streaming di contenuti multimediali e simili, a meno che non si tratti di siti riconducibili all'attività lavorativa.

3.2 Utilizzo del PC

In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, l'utente non deve lasciare il sistema operativo del proprio pc aperto e deve provvedere a proteggere il proprio computer attraverso la sospensione o il blocco della sessione di lavoro.

Al termine dell'orario di servizio, prima di lasciare gli uffici, deve assicurarsi di avere opportunamente spento il proprio PC.

L'utente è responsabile del PC portatile e/o eventuali accessori a lui assegnati (macchina fotografica, videoproiettore) e deve custodirli con diligenza, sia all'interno degli uffici, sia durante gli spostamenti esterni, fino alla loro riconsegna. Particolare attenzione deve essere prestata nell'utilizzo e nella custodia del PC portatile al di fuori della rete e degli uffici dell'Ente, (ad es. in telelavoro) nella connessione a reti esterne e nella rimozione di eventuali file personali memorizzati nel medesimo prima della riconsegna.

3.3 Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali ecc…) è riservato esclusivamente all'attività lavorativa. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

4) Sicurezza e Privacy

Nell'utilizzo delle strumentazioni informatiche occorre adottare le seguenti cautele:

a. mantenere segrete le proprie credenziali di autenticazione (*password*), sia quelle d'accesso alla strumentazione in dotazione sia quelle d'accesso ai vari programmi utilizzati nell'ambito della propria attività lavorativa, attribuite dal Responsabile del Sistema Informatico;
b. non cedere, una volta autenticati nel proprio pc, l'uso della propria postazione a persone non autorizzate, in particolare per l'accesso ad internet ed ai servizi di posta elettronica;
c. adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la sicurezza dei dati trattati e dei dati che possono fornire indicazioni utili ad un eventuale "*hacker*" (attaccante dei sistemi informativi) dell'Azienda;
d. utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dall'Azienda al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali, grazie al sistema centralizzato di *backup*;
e. prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su *file server*);
f. non connettere alla rete interna dell'Azienda apparati esterni (come ad es. *modem* o *router…*) che possano compromettere il corretto funzionamento della rete aziendale;
g. non utilizzare strumenti di messaggistica istantanea (per es. Skype, Messenger) per motivi personali;
h. non introdurre o diffondere nella rete aziendale programmi illeciti (per es. virus, worm, spyware,...) ;
i. non compiere azioni in violazione delle norme a tutela delle opere dell'ingegno e/o del diritto d'autore;

j. utilizzare la posta elettronica messa a disposizione dell'ente per lo svolgimento dell'attività lavorativa, esclusivamente per le specifiche finalità della stessa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
k. non utilizzare *mail* esterne in *software* di posta elettronica (es. Outlook Express), in quanto le stesse comportano rischi per la sicurezza dei sistemi, mentre è consentito l'utilizzo a fini privati di *mail* esterne via web (es. googlemail, poste.it, alice…), purché con moderazione e per brevi periodi di tempo;
l. aver cura di non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire i rischi causati da *software* nocivi (per es. virus, worm, spyware, ecc.);
m. limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail istituzionale su siti web pubblici (per es. forum, mailing list, ecc.);
n. non rimuovere il programma antivirus installato sulla postazione di lavoro;
o. verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili;
p. nel caso in cui il *software* antivirus rilevi la presenza di un virus sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'evento all'assistenza informatica; non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti;
q. utilizzare sulle postazioni di lavoro esclusivamente il *software* autorizzato e fornito dall'Azienda; eventuali *software* aggiuntivi, rispetto all'installazione standard, dovranno essere richiesti al proprio responsabile;
r. non lasciare incustoditi i dispositivi mobili aziendali (come ad esempio i cellulari e i tablet aziendali);
s. in caso di incidente di sicurezza (come ad esempio nei casi di accesso non autorizzato o di minacce informatiche al sistema), attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi;
t. Nell'utilizzo della posta elettronica certificata, le credenziali (user id e password) per accedere a tale casella di posta devono essere a conoscenza unicamente dei collaboratori dell'ufficio autorizzati dal responsabile del servizio.

Per quanto riguarda i collaboratori addetti al Sistema Informativo Aziendale, in ragione delle funzioni svolte, ad essi non si applicano i punti 3.1d, 4.q .

5. Controlli

L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.

I controlli vengono effettuati dal Responsabile della sicurezza con l'ausilio dell'assistenza tecnica, anche dietro segnalazione proveniente dalle strutture regionali competenti o dagli organi di polizia giudiziaria.

5.1 Principi

L'Azienda ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Si impegna pertanto a potenziare in misura crescente tale attività di prevenzione, in particolare tramite azioni di sensibilizzazione e di diffusione dei principi e delle regole da osservare nell'utilizzo della strumentazione informatica, nell'adozione di specifiche soluzioni tecnologiche e di ogni altra misura ritenuta idonea a tal fine.

I controlli effettuati dall'Azienda rispettano i seguenti principi:

a) necessità: i dati trattati durante l'attività di controllo sono sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 5.2;
b) proporzionalità: i controlli sono sempre effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate al paragrafo 5.2;
c) imparzialità: i controlli sono effettuati su tutta la strumentazione informatica messa a disposizione dall'amministrazione aziendale e conseguentemente possono coinvolgere tutti i collaboratori della stessa, a qualunque titolo utilizzino tale strumentazione, fatta eccezione per quella assegnata alle rappresentanze sindacali unitarie e agli organi istituzionali. In nessun caso sono effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie;
d) trasparenza: in base a tale principio l'amministrazione mette in atto tutte le azioni necessarie a garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente regolamento. Sono pertanto informati dei possibili controlli tutti i soggetti di cui al precedente punto 2);
e) protezione dei dati personali: i controlli sono in ogni caso effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo, nonché garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati sono conosciuti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. Oltre a quanto specificato sopra, i controlli sono effettuati rispettando la normativa vigente in materia di protezione dei dati personali.

5.2 Finalità

I controlli di cui al presente regolamento sono effettuati per le seguenti finalità:

a) evitare che vengano compiuti comportamenti impropri e/o potenzialmente dannosi per l'Amministrazione che possano comportare anche l'irrogazione di sanzioni disciplinari;
b) evitare o comunque ridurre i rischi di un coinvolgimento civile e penale dell'Azienda, per concorso di reato, nel caso di illeciti nei confronti di terzi commessi mediante l'utilizzo improprio dei beni messi a disposizione dall'Amministrazione stessa;
c) tutelare l'immagine dell'Azienda e di coloro che vi prestano la propria attività.

5.3 Modalità di effettuazione dei controlli

Il controllo è effettuato su strumentazioni informatiche determinate a seguito di specifica **segnalazione** effettuata da un soggetto terzo oppure a seguito ad una **verifica di sicurezza.**

Nel caso in cui la *segnalazione del soggetto terzo* si riferisca a una persona nominativamente individuata, il Responsabile della sicurezza dell'Azienda deve dare informazione di tale controllo al a tale soggetto, specificando che quest'ultimo può presentare richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990 e ss. mod. e int.

Le segnalazioni di un soggetto terzo sono ritenute più attendibili qualora non siano anonime e rivolte per iscritto al Responsabile della sicurezza.

La *verifica di sicurezza* consiste in una attività di controllo da parte del Responsabile della sicurezza, il quale, dopo aver rilevato elementi che possano configurare un utilizzo improprio delle strumentazioni informatiche, anche mediante ulteriori accertamenti, comunica i dati strettamente necessari, acquisiti attraverso tale controllo, al Responsabile dell'Ufficio di appartenenza del

collaboratore interessato. Quest'ultimo potrà effettuare le ulteriori valutazioni e adottare le azioni conseguenti.

Gli ulteriori accertamenti sopraindicati possono ricomprendere controlli sui *log* (siti di navigazione in Internet). E' possibile verificare il contenuto dei siti di navigazione soltanto nel caso in cui le relative informazioni siano indispensabili al fine di rilevare un utilizzo proprio o improprio dello strumento informatico.

Qualora, anche a seguito delle ulteriori verifiche effettuate, il Responsabile della sicurezza riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dall'Azienda, associa il nominativo dell'utilizzatore alla postazione *client*, per poter procedere come di seguito disciplinato.

Conseguentemente alle verifiche sopraindicate e all'individuazione del nominativo dello/degli utilizzatore/i, il Responsabile della sicurezza:

- trasmette al dirigente di riferimento del soggetto coinvolto un "**Verbale di controllo**" affinché il dirigente stesso possa effettuare le valutazioni conseguenti, con particolare riferimento ad una verifica relativa alla pertinenza (o stretta attinenza) dei dati di navigazione, trasmessi nel Verbale stesso, con l'attività lavorativa;
- ne dà contestuale comunicazione al soggetto coinvolto.

La verifica di pertinenza con l'attività lavorativa, effettuata dal dirigente di riferimento, deve comprendere anche una tempestiva audizione del soggetto controllato, affinché quest'ultimo possa fornire chiarimenti, motivazioni ed osservazioni in merito a quanto rilevato. Alla audizione può essere presente, su richiesta del dirigente di riferimento o del soggetto coinvolto nel controllo, il Responsabile della sicurezza (o altro tecnico addetto alla sicurezza individuato dal Responsabile della sicurezza).

A seguito delle verifiche sopra specificate, il dirigente comunica immediatamente per iscritto all'utilizzatore l'esito del controllo e adotta nel contempo le opportune misure tecniche/organizzative per evitare il ripetersi del comportamento anomalo, richiamandolo, qualora emergano sue responsabilità. Nel caso in cui dall'accertamento emerga un uso gravemente improprio della strumentazione informatica, il dirigente avvia il conseguente procedimento disciplinare.

§ § §

2. Norme comportamentali rivolte agli studenti ospiti delle residenze universitarie di ER.GO

Premessa

La connettività negli studentati è offerta dietro il rilascio da parte di ER.GO di credenziali di accesso. Le credenziali possono essere utilizzate in tutti gli studentati ER.GO, fatta eccezione per la sede di Ferrara, in cui la connettività è attualmente gestita in outsourcing.

Requisito fondamentale per il rilascio delle credenziali è lo status dell'utente (studente assegnatario/ospite temporaneo).

Per il rilascio delle credenziali lo studente può operare autonomamente (inviando un SMS oppure accedendo ad ABITARE ER.GO), rivolgersi alla portineria ed, in casi particolari, ad ER.GO.

Poiché ad ogni struttura è attribuito un unico indirizzo IP pubblico (registrato a nome di ER.GO/Lepida), l'Azienda ha implementato un servizio proxy, cioè, un servizio che consente la navigazione internet filtrata e tracciata, impedendo agli studenti l'accesso a siti elencati in apposite "liste nere" (c.d. blacklist) universalmente riconosciute e rinvenibili in rete, onde prevenire un uso improprio della navigazione, fornita per scopi didattici.

I log (tracciati) di navigazione degli studenti, conservati per un periodo pari a 6 mesi, possono essere messi a disposizione dell'Autorità Giudiziaria in caso di formale richiesta per esigenze connesse allo svolgimento di attività investigative.

Per motivi di sicurezza, inoltre, le porte di comunicazione (TCP/UDP) sono chiuse, fatta eccezione, ovviamente per quelle che consentono la normale navigazione web e l'uso della posta elettronica.

E' fatta salva, tuttavia, la possibilità per lo studente di ottenere l'apertura di porte specifiche verso determinati indirizzi IP o lo sblocco di siti web, dietro presentazione di una richiesta adeguatamente motivata rivolta al S.I.A. di ER.GO attraverso i canali di comunicazione attivati dall'Azienda (SCRIVICI, ASSISTENZA LIVE…).

All'interno del Regolamento generale delle residenze universitarie di ER.GO è inserito un articolo espressamente dedicato al "servizio di accesso alla rete informatica" che viene fornito agli studenti ospiti.

In questo articolo sono illustrati i comportamenti richiesti agli studenti per garantire la sicurezza informatica.

ARTICOLO 9

(Servizio di accesso alla rete informatica)

1. Presso le residenze universitarie è possibile l'accesso alla rete informatica prevalentemente per motivi didattici.
2. L'accesso è subordinato all'utilizzo di username e password personali. Questi dati sono strettamente personali ed è vietato cederli ad altri ospiti.
3. È vietato:
- utilizzare il servizio informatico per scaricare o visualizzare in streaming materiale coperto da copyright;
- accedere a siti illegali;
- mettere in condivisione o scaricare file tramite programmi *peer to peer* (emule, torrent, ecc.)*;
- utilizzare il proprio dispositivo come hotspot per concedere la connessione internet ad altri studenti**.
4. Nel caso di violazioni alle disposizioni di cui ai commi 2 e 3 ER.GO si riserva la facoltà di sospendere l'account per la navigazione internet.
5. Gli accessi ad internet vengono registrati e conservati per un periodo di almeno sei mesi. I dati relativi agli accessi possono essere forniti su richiesta dell'Autorità Giudiziaria per lo svolgimento di attività d'indagine su illeciti amministrativi e/o penali.

* *Peer to peer*: si fa riferimento ad un tipo particolare di software che permette di scambiarsi file fra utenti collegati a Internet;

** *Hotspot*: si dice di computer collegato allo snodo di una rete telematica che ospita un sito web o altri dati di proprietà di terzi.

§ § §

3. Regolamento per il corretto utilizzo dei *social media* di ER.GO

3.1. L'utilizzo dei *social media* da parte di ER.GO

ER.GO utilizza i social media per informare, comunicare, ascoltare, favorire la partecipazione, il confronto e il dialogo con i propri utenti.

In particolare, attraverso i social media, ER.GO diffonde informazioni su servizi, eventi, progetti, azioni di coinvolgimento e partecipazione; può inoltre diffondere aggiornamenti in situazioni di emergenza.

L'elenco aggiornato dei social media su cui è presente ER.GO è disponibile nella Home page del sito istituzionale www.er.go.it.

I social media non sostituiscono, ma affiancano l'attività di comunicazione/informazione svolta attraverso il portale www.er.go.it o tramite i servizi interattivi ad esso collegati (DOSSIER / SCRIVICI / ABITARE ER.GO / ASSISTENZA LIVE).

3.2. Gestione dei *social media*

Gli account (pagine e profili) istituzionali di ER.GO sui social network sono gestiti per conto dell'Azienda da una società specializzata, con il coordinamento del Servizio Comunicazione.

La presente **social media policy esterna** definisce e descrive le essenziali regole di comportamento che gli utenti sono tenuti ad osservare quando interagiscono con le pagine e i profili istituzionali di ER.GO sui social network.

3.3. Contenuti pubblicati sui *social network*

I contenuti pubblicati sui social media provengono da ER.GO, se non indicato diversamente da quest'ultima.

ER.GO, attraverso i suoi organi di direzione, oltre a garantire la correttezza dei contenuti pubblicati in termini di legittimità e liceità, è impegnata ad assicurare la qualità delle informazioni pubblicate sui propri canali social, nonché la loro integrità, aggiornamento, completezza, tempestività, semplicità di consultazione e accessibilità.

ER.GO può condividere occasionalmente contenuti e messaggi di terze parti (altri enti, es. le Università, o persone) ritenuti di pubblico interesse e utilità. In questo caso, fermo restando l'impegno nel verificare la precisione e l'attendibilità di questi contenuti, ER.GO non si assume alcuna responsabilità per eventuali informazioni errate e non aggiornate.

L'aggregazione ad opera di terzi dei contenuti pubblicati da ER.GO con contenuti pubblicati da altri soggetti, così come eventuali rielaborazioni di quanto pubblicato da ER.GO non sono sotto il controllo di quest'ultima.

3.4. Comportamenti consentiti/non consentiti agli utenti

I contenuti pubblicati da ER.GO possono essere condivisi, commentati e utilizzati dagli utenti:

- nel rispetto dei termini di servizio di ogni piattaforma di social media;
- nel rispetto della normativa vigente.

Gli utenti che interagiscono con gli account istituzionali di ER.GO sui social network sono invitati ad identificarsi con nome e cognome. Nel caso di utilizzo di nomi fittizi (nickname) gli amministratori valutano se nell'ambito della discussione ci siano validi motivi per mantenere la condizione di anonimato; qualora tali motivi non sussistano, i post e/o i commenti anonimi saranno rimossi.

In particolare, si indicano i comportamenti consentiti per i seguenti social media:

Facebook

Gli utenti che interagiscono con la pagina (*fan page*) di ER.GO su Facebook possono:

• apprezzare i contenuti (post) pubblicati nella bacheca di ER.GO cliccando "Mi Piace";

• commentare i contenuti (post) pubblicati nella bacheca di ER.GO (notizie, fotografie, video, eventi e link);

• condividere nella propria bacheca i contenuti (post) pubblicati nella bacheca di ER.GO;

• inviare messaggi privati dal proprio account personale alla pagina di ER.GO.

Agli utenti Facebook non è consentito pubblicare autonomamente contenuti nella bacheca della pagina istituzionale di ER.GO.

Twitter

Gli utenti che interagiscono con il profilo istituzionale di ER.GO su Twitter possono:

• scrivere, utilizzando il proprio account personale, messaggi pubblici (tweet) destinati ad ER.GO (non è necessario seguire assiduamente, cioè essere un "follower" di ER.GO);

• scrivere, utilizzando il proprio account personale, messaggi privati all'account di ER.GO (è necessario essere follower di ER.GO);

• inoltrare ("ritwittare") ai propri follower i messaggi (tweet) pubblicati da ER.GO con il proprio account istituzionale.

ER.GO chiede ai propri utenti/interlocutori il rispetto di alcune regole basilari:

1. a tutti si chiede di esporre la propria opinione con correttezza e misura, basandosi per quanto possibile su dati di fatto verificabili, e di rispettare le opinioni altrui.
2. nei social network ognuno è responsabile dei contenuti che pubblica e delle opinioni che esprime. Non saranno tollerati insulti, volgarità, offese, minacce e, in generale, atteggiamenti violenti, comportamenti gratuitamente polemici, tenuti soltanto per disturbare, creare confusione e provocare litigi, soprattutto se reiterati (c.d. *trolling* o *flame);*
3. i contenuti pubblicati devono rispettare sempre la privacy delle persone. Vanno evitati riferimenti a fatti o a dettagli privi di rilevanza pubblica o che ledano la sfera personale di terzi.
4. l'interesse pubblico degli argomenti è un requisito essenziale: si invitano gli utenti ad utilizzare i servizi interattivi disponibili sul sito ER.GO (DOSSIER / SCRIVICI / ABITARE ER.GO / ASSISTENZA LIVE) per affrontare casi personali.
5. non sono ammessi i seguenti comportamenti: promozioni di prodotti, spam, inserimento di link a siti esterni fuori argomento (c.d. *off topic*), promozione di interessi privati o di attività illegali.
6. non sono ammessi contenuti che violino il diritto d'autore; non è ammesso l'utilizzo non autorizzato di marchi registrati.
7. non è ammessa la promozione di raccolta fondi.

In ogni caso, ove i social media lo permettano, saranno rimossi tutti i post, i commenti o i materiali audio/video che:
* presentano un linguaggio inappropriato e/o un tono minaccioso, violento, volgare o irrispettoso;
* presentano contenuti illeciti o di incitamento a compiere attività illecite;
* hanno contenuti offensivi, ingannevoli, allarmistici, o in violazione di diritti di terzi;
* divulgano dati e informazioni personali o che possono cagionare danni o ledere la reputazione di terzi;
* presentano contenuti di carattere osceno, pornografico o pedopornografico, o tale da offendere la sensibilità degli utenti;
* hanno un contenuto discriminatorio per genere, razza, etnia, lingua, credo religioso, opinioni politiche, orientamento sessuale, età, condizioni personali e sociali.

3.5. Moderazione

La moderazione da parte di ER.GO all'interno dei propri spazi avviene a posteriori, ovvero in un momento successivo alla pubblicazione, ed è finalizzata unicamente al contenimento, nei tempi e nei modi ragionevolmente esigibili, di eventuali comportamenti contrari alle norme d'uso.

Nei casi più gravi – e in particolare in caso di mancato rispetto delle regole condivise in questo documento - gli amministratori degli account istituzionali di ER.GO sui social network hanno la facoltà di eliminare, senza alcun preavviso, i contenuti non conformi.

A seguito di reiterati comportamenti con rispettosi delle regole descritte, l'utente responsabile potrà essere bloccato ("bannato") per impedire ulteriori interventi e segnalato ai filtri di moderazione del social network ospitante ed eventualmente alle autorità competenti.

ER.GO si riserva di segnalare eventuali casi di violazione della proprietà intellettuale o di abuso dell'identità e dell'immagine di ER.GO anche attraverso account falsi (fake) ai gestori delle piattaforme e, se necessario, alle autorità competenti.

Gli spazi social di ER.GO vengono presidiati, di regola, dal lunedì al venerdì. ER.GO si impegna a leggere i messaggi e a fornire, qualora richiesta, una risposta. Qualora i canali social non siano lo strumento adeguato per soddisfare la richiesta, il gestore provvederà ad informare sulle corrette modalità e uffici a cui rivolgersi.

3.6. Protezione dei dati personali

Si ricorda che il trattamento dei dati personali degli utenti risponde alle policy in uso sulle piattaforme utilizzate (Twitter, Facebook, etc.) Si rammenta che i dati sensibili postati in commenti o post pubblici all'interno dei canali social verranno rimossi.

I dati personali condivisi dagli utenti attraverso messaggi privati spediti direttamente ad ER.GO saranno trattati nel rispetto del decreto legislativo 30 giugno 2003, n. 196 e successive modifiche e integrazioni.

Il titolare del trattamento è:

ER.GO Azienda Regionale per il Diritto agli Studi Superiori
C.F.02786551206
Via Santa Maria Maggiore, 4
40121 BOLOGNA.

Il responsabile del trattamento è il Direttore di ER.GO (direzione@er-go.it; PEC: info@postacert.er-go.it; tel. 051/6436742-45,).