# REGOLAMENTO INFORMATICO

## Sommario

## 1. INTRODUZIONE

La garanzia della riservatezza, dell'integrità e della disponibilità dei sistemi e dei dati informatici di IUSTO è un obiettivo vitale per l'ente. Il presente regolamento descrive le *norme* (2) e gli *standard* (3) di utilizzo appropriato dei *Sistemi Informatici* di IUSTO, definendo quanto costituisce un uso accettabile di tali sistemi e quali attività sono invece proibite.

### DEFINIZIONI

***Sistemi Informatici*** (o per brevità ***Sistemi***): qualsiasi computer, laptop, PDA, tablet, smartphone, LIM, server, rete, switch, cavo e in generale qualsiasi dispositivo elettronico fornito o supportato da IUSTO, ovunque esso sia utilizzato. La gestione di tali *Sistemi* comprende l'uso di dati e programmi contenuti sia nei *Sistemi* stessi, sia su qualunque altro strumento di memorizzazione esterno o rimovibile (CD, DVD, blu-ray disc, hard disk, SSD, pen drive, memory card, ecc.) posseduto o conservato da IUSTO.

***Server Aziendali*** (o per brevità ***Server***): i computer, non assegnati specificamente ad uno o più utenti, utilizzati centralmente presso la sede di IUSTO per la gestione delle applicazioni e per la conservazione delle informazioni.

***Servizi in Cloud*** (o per brevità ***Cloud***): i servizi di archiviazione dati gestiti da IUSTO presso data center di terzi collocati fisicamente fuori da IUSTO, per la gestione delle applicazioni e per la conservazione delle informazioni.

**Utente**: qualsiasi persona che abbia un account di sistema IUSTO o un hardware (o entrambi), fornitogli allo scopo di svolgere del lavoro a supporto dell'attività di IUSTO o di effettuare un percorso formativo da esso erogato. La definizione di Utente si distingue in:

a) **Collaboratore**: l'Utente che collabori con IUSTO, avendo con esso un qualsiasi rapporto di lavoro di tipo subordinato, parasubordinato, occasionale o eserciti per esso un qualsivoglia incarico professionale.
b) **Allievo**: l'Utente iscritto a un qualunque percorso di studi o attività formativa erogata da IUSTO.

**Responsabile *Sistemi Informatici*** (o per brevità ***RSI***): è la persona, nominata dalla direzione aziendale, incaricata di controllare l'applicazione delle Norme e degli Standard di Utilizzo specificati in questo documento.

## 2. NORME GENERALI

Tutti gli ***Utenti*** dei *Sistemi* di IUSTO sono tenuti a osservare le seguenti norme generali.

**Responsabilità per la sicurezza delle informazioni** – Gli *Utenti* dei *Sistemi* informativi di IUSTO condividono con l'ente la responsabilità per la protezione dei dati e devono agire di conseguenza. Gli *Utenti* non devono conservare dati personali di terzi senza una precisa giustificazione. Gli *Utenti* non devono effettuare copie non autorizzate di dati e non devono trasmettere alcun dato a terzi senza idonea autorizzazione.

**Comunicazione di difetti ed incidenti** – Gli *Utenti* devono riferire al *RSI* qualsiasi punto di debolezza riscontrato nella funzionalità o nella sicurezza dei *Sistemi Informatici* di IUSTO, nonché qualsiasi incidente o anomalia di funzionamento relativi a *Sistemi* o dati aziendali.

**Archiviazione e conservazione delle informazioni** – Tutte le informazioni contenute nei *Sistemi* di IUSTO devono essere immagazzinate e conservate in conformità alle esigenze e politiche aziendali ed ai requisiti legislativi e regolamentari applicabili.

**Accesso ai Sistemi** – I *Sistemi Informatici* di IUSTO sono protetti da password. Gli *Utenti* non devono conservare le proprie credenziali di accesso su supporti cartacei o digitali accessibili a terzi, né rivelare o condividere le password con nessuno.

**Diritto d'autore** – Tutti i software e le applicazioni utilizzate nei *Sistemi* di IUSTO sono coperti da licenze e contratti sul diritto d'autore. Gli *Utenti* devono osservare le norme che disciplinano tali licenze. I software privi di licenza non devono essere utilizzati nei *Sistemi* di IUSTO.

**Hardware** – È vietata qualunque modifica hardware che non sia espressamente autorizzata dal *RSI* e svolta da lui o sotto la sua supervisione. Gli *Utenti* non possono utilizzare né collegare ai *Sistemi Informatici* aziendali apparecchiature hardware di loro proprietà, se non in via del tutto eccezionale e acquisito il consenso scritto del *RSI*.

**Software** – Solo i software approvati da IUSTO devono essere utilizzati sui computer di IUSTO. Gli *Utenti* non devono introdurre software aggiuntivi senza l'approvazione dell'ente e non devono conservare nei *Sistemi* di IUSTO materiale che non sia giustificato dall'attività dell'azienda.

**Stampanti multifunzione e fotocopiatrici** – L'utilizzo delle stampanti multifunzione e delle fotocopiatrici è consentito agli *Utenti* autorizzati solo mediante codice di accesso personale o altro identificativo univoco.

**Virus** – Gli *Utenti* non devono disabilitare i software anti-virus e devono assicurarsi che tutti i file elettronici siano stati controllati dall'antivirus prima del loro utilizzo.

**Posta elettronica** – I servizi di posta elettronica sono esclusivamente destinati ad un uso lavorativo e professionale nell'interesse di IUSTO e devono essere utilizzati di conseguenza. Messaggi e materiali contrari a norme di legge, offensivi o osceni non devono essere inviati o conservati sui *Sistemi* di IUSTO.

**Internet** – I servizi internet sono destinati esclusivamente all'uso professionale di IUSTO e devono essere utilizzati di conseguenza.

**Social media e messaggi** – L'utilizzo dei social media e dei sistemi di messaggistica non è vietato o impedito agli *Utenti*, purché avvenga nel rispetto delle regole definite all'interno di questo documento.

**Rilevazione presenze** – La rilevazione della presenza in aula di *Allievi* e *Collaboratori* docenti avviene normalmente tramite badge personale. Gli *Utenti* non devono consentire a nessun altro di utilizzare il proprio badge, né utilizzare un badge altrui. La simulazione dell'identità di un altro *Utente* costituisce grave illecito e dà luogo a sanzioni disciplinari.

**Dati Personali** – Tutti i dati personali in possesso di IUSTO devono essere trattati con correttezza, secondo i principi etici ed in sicurezza, conformemente al Regolamento UE 2016/679.

**Monitoraggio** – IUSTO ha il diritto di condurre monitoraggi periodici dei propri *Sistemi Informatici* e del loro uso per assicurarne la conformità al presente regolamento. Ciò avverrà nel pieno rispetto dei diritti degli *Utenti*, in conformità a tutte le disposizioni di legge e regolamentari applicabili e, in particolare, delle linee guida stabilite in materia dal garante per la protezione dei dati personali con la deliberazione n. 13 del 1 marzo 2007 e s.m.i.

**Disabilitazione e cancellazione degli account** – IUSTO ha il diritto di procedere alla disabilitazione ed alla cancellazione degli account inutilizzati nel rispetto delle sopracitate norme e linee guida.

**Rispetto della Legge** – L'uso e la gestione di tutti i servizi informatici di IUSTO devono avvenire nel pieno rispetto delle norme e dei regolamenti localmente applicabili.

Qualsiasi mancato rispetto di tali indicazioni può comportare l'irrogazione di sanzioni disciplinari.

## 3. STANDARD DI UTILIZZO APPROPRIATO DEI SISTEMI INFORMATICI DI IUSTO

Le sezioni seguenti disciplinano in dettaglio gli standard a cui tutti gli *Utenti* devono adeguarsi.

### A. Responsabilità per la sicurezza delle informazioni

Gli *Utenti* dei *Sistemi* sono corresponsabili della protezione dei dati memorizzati sui *Sistemi* medesimi.

Qualsiasi violazione della sicurezza delle informazioni può determinare una perdita di informazioni vitali ed i danni causati a IUSTO possono essere rilevanti. Tali violazioni possono anche esporre le persone fisiche responsabili ad azioni legali.

Gli *Utenti* si assicureranno che:

- I dati personali relativi a terzi non siano conservati senza una precisa giustificazione o senza che ne sia data comunicazione agli organi a ciò deputati (i superiori gerarchici e/o il titolare del loro trattamento);
- I dati conservati nei Server Aziendali non vengano eliminati (ad esempio, cancellati o spostati dall'area di archiviazione designata) senza approvazione, alterati senza autorizzazione o rivelati a persone non autorizzate.
- Siano adottate tutte le misure concrete per tutelare la proprietà intellettuale di IUSTO nel rispetto della normativa sulla protezione della proprietà intellettuale e, in particolare, del D. Lgs. 30/2005.
- Siano adottate tutte le misure concrete per assicurarsi che l'attrezzatura informatica appartenente a IUSTO non venga rubata o danneggiata.
- Siano adottate tutte le misure concrete per assicurarsi che le attrezzature portatili (compresi laptops, computer palmari, tablet e smartphones) siano conservate in modo sufficientemente sicuro (ad esempio chiusi nel bagagliaio se lasciati incustoditi in un'automobile, trasportati in apposite borse, etc.) e che, quando e ovunque tali attrezzature vengano utilizzate, siano seguiti tutti gli standard elencati in questo documento.
- Il materiale informatico non sia spostato (salvo che tale attrezzatura non sia designata come portatile), né sia installato alcun nuovo strumento informatico, senza l'autorizzazione sia da parte del superiore gerarchico sia da parte del *RSI*.
- Nessun computer portatile o fisso, aziendale, personale oppure posseduto da altra persona o altra società, sia installato o utilizzato, nei locali aziendali o in altri luoghi dove ci sia una attività lavorativa di personale e/o *Sistemi* IUSTO, senza seguire gli standard elencati in questo documento.
- L'accesso alle reti aziendali, sia in sede che ovunque installate, deve essere autorizzato sia da parte del superiore gerarchico sia da parte del *RSI* e deve essere gestito da personale del reparto informatico.
- Il materiale informatico deve essere spento al termine di ogni giorno, salvo che l'apparecchio debba restare in attività continua.
- I dati aziendali devono essere archiviati nei *Server Aziendali* nelle aree a ciò deputate, non sul proprio desktop, in *hard disk* locali né in *pendrive* USB, dal momento che questi non sono sicuri o soggetti a *backup* automatico.
- Non devono essere effettuate copie non autorizzate dei dati aziendali; l'eventuale autorizzazione va richiesta in forma scritta alla direzione. Nel caso in cui sia necessaria una copia autorizzata, gli *Utenti* devono assicurarsi che, qualsiasi sia il mezzo utilizzato (CD-ROM, chiave di memoria USB, hard-disk portatile, smartphone, tablet, ecc.), venga archiviato in sicurezza quando non in uso.
- I dati non devono essere trasmessi a terzi senza espressa e specifica autorizzazione, a meno che non si tratti di una operazione necessaria nel contesto dell'attività lavorativa.
- Tutti i file forniti a IUSTO da terzi vengano scansiti per controllo anti-virus prima dell'installazione nei *Sistemi*.
- I materiali osceni, pornografici, razzisti, di carattere sessuale o diffamatori non devono essere copiati o archiviati nei *Sistemi* di IUSTO, fatto salvo un loro eventuale uso che potrà essere autorizzato solo per comprovati motivi di studio o di ricerca.
- Qualsiasi uso dei *Sistemi* per archiviare materiali personali, non legato all'attività aziendale, sia strettamente limitato e temporaneo.

### B. Comunicazione di difetti ed incidenti

Gli *Utenti* devono riferire appena possibile al *RSI*, mediante l'apertura di un ticket su *https://assistenza.ius.to/*, qualsiasi punto di debolezza o di vulnerabilità nella sicurezza dei *Sistemi* di IUSTO; lo stesso vale per qualsiasi incidente o possibile uso improprio, furto o perdita di dati o di *Sistemi* appartenenti a IUSTO.

Il furto o lo smarrimento di attrezzature deve anche essere immediatamente comunicato alla direzione e denunciato all'autorità di pubblica sicurezza, dalla quale dovrà anche essere ottenuta copia della denuncia.

## C. Archiviazione e conservazione delle informazioni

Tutte le informazioni detenute nei *Sistemi* devono essere archiviate e conservate in conformità alla politica aziendale e alle altre norme legislative e regolamentari applicabili e in particolare, ove si tratti di dati personali, al Regolamento UE 2016-679. Gli *Utenti* devono essere consapevoli che:

- la tenuta di informazioni in formato elettronico comporta il consumo di risorse, sia in termini di archiviazione di dati, che di risorse umane per la gestione di tali archivi; gli *Utenti*, nel caso in cui ritengano che informazioni irrilevanti e non aggiornate siano conservate senza necessità, devono provvedere, se ne hanno facoltà, alla cancellazione di dati obsoleti o ridondanti; non disponendo di tali permessi, sono comunque tenuti ad informare il loro diretto superiore e il *RSI* affinché vengano presi gli opportuni provvedimenti;
- i dati e i documenti devono essere archiviati nelle apposite cartelle (predisposte da IUSTO in ragione delle diverse aree e funzioni organizzative) sui *Server* o nel *Cloud*.
- i *Server Aziendali* non devono essere utilizzati per archiviare i dati di proprietà degli *Utenti* (ad esempio, lettere, immagini e documenti personali). I *Collaboratori* possono richiedere al *RSI* un apposito spazio, che sarà creato dal *RSI* stesso e denominato con nome e cognome del dipendente, sul quale archiviare dati non aziendali; tale spazio non potrà superare la dimensione di 500Mb, a meno che non sia espressamente autorizzato dalla direzione aziendale;
- i dati personali possono essere archiviati localmente nei *Sistemi* messi dall'azienda a disposizione dell'utente e nello spazio di cui al punto precedente tenendo in considerazione quanto dettagliato nella sezione O (*Monitoraggio*) di questo documento.

Il *RSI* predispone, d'intesa con la direzione, delle linee guida specifiche in merito, che provvede a rendere note agli *Utenti* interessati mediante pubblicazione in apposita area.

Nel caso di dubbi o incertezze circa la corretta archiviazione e conservazione di dati, gli *Utenti* si devono rivolgere al *RSI*.

## D. Accesso ai Sistemi

I *Sistemi* sono protetti da password come sistema di protezione principale contro l'accesso non autorizzato. L'uso di password è attentamente controllato e gli *Utenti* devono conformarsi a quanto segue:

- Le password non devono essere rivelate a nessuno e non devono essere accessibili a persone non autorizzate.
- In circostanze eccezionali, quali ad esempio periodi di malattia o di assenza, e solo con l'approvazione della direzione al *RSI* può essere fatta richiesta di consentire al superiore gerarchico di accedere ai dati aziendali detenuti dall'utente stesso. In tal caso, le password devono essere sostituite di nuovo non appena possibile quando l'utente torna al lavoro.
- Gli *Utenti* non devono scegliere password che siano ovvie o facilmente immaginabili in quanto riconducibili a propri dati personali (ad es. nomi e cognomi, date di nascita, numeri di telefono, indirizzi e-mail, ecc.) o modificare le password con variazioni simili (ad esempio, da IUSTO1 a IUSTO2). Inoltre, le password devono avere una lunghezza di almeno 8 caratteri e devono contenere lettere maiuscole e minuscole, numeri e caratteri speciali (es. { } [ ] , . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _.-).
- Nel caso si abbia il dubbio che una password non sia più "sicura", occorre cambiarla immediatamente.
- Le password non devono essere memorizzate su alcun tipo di supporto che può essere visto o utilizzato da altri, quali, ad esempio, post-it (sul monitor o sotto la tastiera) o agende (fisiche o digitali).
- Le password devono essere sostituite almeno una volta ogni tre mesi o in base alle indicazioni del sistema automatico di richiesta di aggiornamento password, se presente.
- Occorre evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente.

Non deve essere effettuato alcun tentativo di accesso ai *Sistemi* o ai dati senza idonea autorizzazione.

In alcuni casi, possono essere presenti meccanismi che consentono un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene automaticamente bloccato per un tempo determinato. In tal caso, gli *Utenti* devono contattare il *RSI*.

Gli *Utenti* non devono tentare di ottenere accessi ulteriori rispetto a quelli attribuiti o provare ad aggirare le misure di sicurezza informatiche di IUSTO. Eventuali tentativi in tal senso saranno perseguiti a norma di legge.
IUSTO si riserva il diritto di modificare le password e di accedere ai dati negli account individuali, laddove ciò sia necessario al fine di assicurare l'osservanza delle norme di legge e delle regole di condotta aziendale e, in ogni caso, fermo il rispetto delle vigenti disposizioni sulla privacy.

### E. Diritto d'Autore

Tutti i software e le applicazioni utilizzate nei *Sistemi* sono coperti da licenze e contratti sul diritto d'autore e gli *Utenti* devono osservare tali licenze e i contratti relativi ai software che utilizzano. In particolare:

- I software protetti da licenza d'uso non devono essere installati o utilizzati nei *Sistemi* in mancanza di tale licenza.
- Tutte le licenze, i contratti, i contratti di manutenzione e gli altri documenti contrattuali sui *Sistemi* devono essere trasmessi al *RSI* e non trattenuti dagli *Utenti* finali.

Tutti i dati, i documenti, le applicazioni e software sviluppati o redatti dai *Collaboratori* nel corso dell'orario lavorativo o sull'attrezzatura di IUSTO restano proprietà di IUSTO.

### F. Hardware

Tutti i componenti hardware dei *Sistemi* di IUSTO devono essere trattati con cura e non devono in alcun caso essere manomessi o modificati. Ai *Collaboratori* docenti è consentito l'uso di supporti di memoria rimuovibili contenenti materiale didattico, previa verifica della loro funzionalità e compatibilità.
Per il resto, è vietata qualunque modifica hardware che non sia espressamente autorizzata dal *RSI* e svolta da lui o sotto la sua supervisione. Gli *Utenti* non possono utilizzare né collegare ai *Sistemi Informatici* aziendali apparecchiature hardware di loro proprietà, se non in via del tutto eccezionale e acquisito il consenso scritto del *RSI*.

### G. Software

Solo i software approvati da IUSTO devono essere utilizzati sui computer di IUSTO. Gli *Utenti* prendono atto che:

- qualsiasi software, sia esso anche un software dimostrativo, installato nei *Sistemi* deve essere autorizzato dal *RSI*;
- qualsiasi software, non freeware, installato nei *Sistemi* deve essere dotato di idonea licenza;
- l'elenco dei software freeware installabili sui PC assegnati agli *Utenti* è redatto e diffuso dal *RSI*, previa autorizzazione della direzione.

### H. Stampanti multifunzione

È attivo un sistema di monitoraggio software delle stampe e delle fotocopie effettuate. Lo scopo di questa operazione è di sensibilizzare gli utenti ad un uso appropriato degli strumenti a disposizione, ridurre l'impatto ambientale e consentire un'ottimizzazione dei costi sostenuti in questo ambito. Al termine di ogni mese, ciascun *Collaboratore*, se previsto, riceve alla sua casella e-mail, un report sulle stampe/fotocopie e scansioni effettuate. Anche per gli *Allievi* è possibile controllare il proprio uso di stampe/fotocopie e scansioni utilizzando il proprio codice di accesso o la propria tessera personale/badge. L'accesso via intranet è disponibile all'indirizzo http://papercut:9191/.
Il report distingue tra stampe a colori e stampe in b/n, tiene conto dell'utilizzo del fronte/retro e notifica il costo totale azienda per tali stampe (esclusa l'energia elettrica). L'uso delle stampanti multifunzione è riservato alle attività di carattere didattico o professionale. L'esecuzione di stampe o fotocopie per esigenze personali deve essere autorizzata dalla direzione e comporta per l'utente il rimborso del costo sostenuto dall'azienda.
Gli *Allievi* possono utilizzare le stampanti multifunzione a loro destinate previa disponibilità di un credito sul proprio badge personale. Essi possono acquistare i codici di ricarica del proprio credito presso la segreteria studenti.

## I. Virus

I virus causano danni ai *Sistemi Informatici*. Gli *Utenti* sono responsabili per qualunque comportamento idoneo a compromettere, in tutto o in parte, la protezione dei dati e dei *Sistemi* contro attacchi da parte di virus. In particolare:

- i software anti-virus non devono essere disabilitati;
- tutti i file derivanti da fonti esterne a IUSTO, ad esempio CD-ROM, chiave di memoria USB o allegati di posta elettronica, devono essere controllati con l'antivirus prima della loro installazione nei *Sistemi*.

Qualsiasi *Utente* che riceva un avviso di virus dovrà richiedere l'assistenza attraverso la piattaforma aziendale di supporto informatico, mediante l'apertura di un ticket su *https://assistenza.ius.to/*.

## J. Posta elettronica

Tutti i *Collaboratori* di IUSTO devono utilizzare la casella di posta elettronica aziendale, contraddistinta dal nome di dominio "@ius.to" o da altri nomi di dominio registrati da IUSTO, come se utilizzassero qualsiasi altro tipo di strumento ufficiale di comunicazione di IUSTO. Non è consentito l'utilizzo dell'indirizzo di posta elettronica fornito dall'azienda per motivi personali se non in via del tutto occasionale, nel rispetto di quanto di seguito indicato e in modo da non interferire con la propria attività lavorativa.
Prima di utilizzare il sistema di posta elettronica interna, gli *Utenti* devono sempre determinare previamente se ciò costituisca la più idonea forma di comunicazione e, in particolare, valutare attentamente l'opportunità di inviare messaggi a liste ed elenchi di distribuzione.
Gli *Utenti* della posta elettronica aziendale, siano essi mittenti o destinatari, devono garantire modalità di comunicazione adeguate e corrette nell'uso di questo strumento. In particolare:

- Gli *Utenti* dei servizi di posta elettronica di IUSTO non devono inviare né archiviare messaggi di posta elettronica contenenti materiale di carattere violento o razzista, osceno o pornografico, minaccioso, molesto, diffamatorio o lesivo dell'immagine; è inoltre severamente vietato inviare in allegato ai messaggi di posta elettronica virus informatici, spyware, malware e qualunque tipo di file pericoloso, dannoso o potenzialmente insicuro (ad es. programmi, script, macro). Infine, gli *Utenti* devono evitare di allegare alle e-mail file di dimensioni eccessive.
- L'uso dei servizi di posta elettronica per scopi che costituiscano un palese conflitto d'interessi con IUSTO, che ne danneggino l'immagine o la reputazione, o che violino i requisisti di sicurezza descritti sopra, è espressamente proibito, in quanto costituisce un uso personale inappropriato della posta elettronica.
- Qualsiasi uso personale dei servizi di posta elettronica deve avere carattere occasionale e non ripetitivo, deve essere il più possibile limitato nel tempo (nell'ordine di pochi minuti), non deve interferire con la normale attività lavorativa, non deve essere associato ad alcuna attività lucrativa esterna, non deve causare imbarazzo per IUSTO; il tempo impiegato per tale uso personale non può essere contabilizzato come tempo di lavoro retribuito.
- Gli *Utenti* che ricevano messaggi di posta elettronica con allegati da fonti sospette o non sicure non devono aprire gli allegati; qualora intendano comunque farlo, devono prima richiedere e ottenere assistenza mediante l'apertura di un ticket su *https://assistenza.ius.to/*.

In tutti i casi, gli *Utenti* non devono consentire a nessun altro di utilizzare il proprio account di posta, né utilizzare account altrui. La simulazione dell'identità di un altro *Utente* costituisce grave illecito.

Potrebbe rendersi necessario, occasionalmente, procedere a controlli sui servizi di posta elettronica degli *Utenti*. Tali operazioni si svolgeranno in ogni caso nel rispetto delle vigenti leggi e norme sulla privacy.

## K. Internet

L'accesso a internet fornito ai *Collaboratori* e agli *Allievi* di IUSTO è uno strumento professionale e culturale importante che consente l'accesso ad un'ampia gamma di informazioni. Tuttavia, l'uso inappropriato di internet

da parte degli *Utenti* potrebbe determinare una situazione di imbarazzo di IUSTO e/o causare azioni legali civili o procedimenti penali contro IUSTO o singoli *Utenti*. Pertanto:

- Tutti gli *Utenti* accedono a internet mediante un sistema di autenticazione personale e non devono accedervi utilizzando l'account di un altro utente.
- Gli *Utenti* ospiti che necessitino di un accesso transitorio a internet riceveranno dal *RSI* delle credenziali temporanee in busta chiusa. Una volta utilizzate, tali credenziali dovranno essere revocate.
- Gli *Utenti* di internet, fatte salve chiare e dimostrabili esigenze di tipo didattico o di ricerca, non possono consultare, trasmettere o scaricare materiali di carattere violento o razzista, osceno o pornografico, minaccioso, molesto, diffamatorio o lesivo dell'immagine.
- Gli *Utenti* di internet non possono scaricare materiale coperto da licenze o protetto da contratti sul diritto d'autore (come, ad esempio, file musicali o film) in violazione della legislazione vigente. Gli *Utenti* devono osservare le norme che disciplinano tali ambiti. Per quanto riguarda il software scaricabile via Internet vale quanto specificato nella sezione G (Software).
- Gli *Utenti* non devono scaricare alcun software autoinstallante da Internet, salvo specifica autorizzazione del *RSI*.
- Gli *Utenti* non devono usare gli strumenti internet forniti da IUSTO per tentare di ottenere accesso non autorizzato ad altri *Sistemi Informatici*.

Oltre a quanto sopra espresso valido per tutti, *Allievi* e *Collaboratori*, questi ultimi devono considerare anche che:

- L'accesso ad internet è concesso ai *Collaboratori*, mediante autenticazione personale, solamente a scopo lavorativo, didattico e professionale. Un eventuale uso personale deve essere assolutamente sporadico e limitato nel tempo, non deve interferire con la normale attività lavorativa, non deve essere associato ad alcuna attività lucrativa esterna: in tutti i casi, il tempo impiegato per tale uso personale non può essere contabilizzato come tempo di lavoro retribuito.
- I *Collaboratori* non devono caricare o pubblicare informazioni in Internet senza preventiva autorizzazione, a meno che non si tratti di una operazione prevista e necessaria nell'ambito della loro ordinaria attività lavorativa.

IUSTO si riserva la possibilità di effettuare dei controlli a campione sull'uso di internet per verificare il rispetto delle sopracitate norme e, ove ne ricorrano le condizioni, adotterà eventuali sanzioni per disciplinare comportamenti non conformi al presente regolamento.

### L. Social media e sistemi di messaggistica

I social media (quali, a puro titolo esemplificativo e non esaustivo, Facebook, LinkedIn, Twitter, Instagram, ecc.), i sistemi di messaggistica personale (quali ad esempio Whatsapp, Telegram, Hangout, ecc.), i professional networking sites, i blog e i siti web personali sono strumenti di comunicazione potenti. IUSTO ne è consapevole ed incoraggia la presenza on-line degli *Allievi* laddove essa possa essere utile come arricchimento professionale e per la condivisione delle conoscenze. Tuttavia, è assolutamente necessario che ogni *Utente* applichi delle regole di prudenza e di buon senso quando sceglie di condividere delle informazioni attraverso questi strumenti.
Ogni *Allievo* è facilmente collegabile a IUSTO e per questo motivo qualsiasi tipo di comunicazione in riferimento a docenti e allievi, clienti e fornitori di IUSTO, nonché in riferimento a IUSTO stessa, non può avere carattere critico, offensivo o lesivo della loro immagine. Per lo stesso motivo, la responsabilità di quanto pubblicato è esclusivamente a carico dell'autore del post. Nel rispetto del punto precedente, gli *Allievi* possono pubblicare qualsiasi opinione, fermo restando che si tratta dell'opinione del singolo e non una forma ufficiale di comunicazione da parte di IUSTO. In ogni caso, IUSTO chiede a tutti gli *Utenti* dei *Sistemi Informatici* aziendali di usare un tono educato e moderato nell'esprimere le proprie opinioni, evitando insulti o parole scortesi verso altre persone, enti o istituzioni.

Per quanto riguarda l'uso dei social media da parte dei *Collaboratori*, esso è da ritenersi proibito durante il tempo lavorativo, a meno che tale uso non rientri esplicitamente tra le mansioni del collaboratore, in quanto incaricato

della comunicazione istituzionale. In particolare, non è consentito accedere ai social media facendo uso di account personali. Gli unici account utilizzabili sono quelli creati appositamente da IUSTO a fini promozionali e comunicativi. I *Collaboratori* che dispongano di account personali di accesso ai Social Media, quand'anche utilizzati in forma privata al di fuori dell'orario di lavoro, sono invitati a ricordare che qualsiasi tipo di post o di comunicazione diffusa sul web che in qualche modo faccia riferimento a colleghi, docenti, allievi, clienti e fornitori di IUSTO, nonché in riferimento a IUSTO stessa, non deve avere carattere offensivo o lesivo della loro immagine.
Ai *Collaboratori* può essere consentito l'uso di social media più specificatamente professionali (ad es. *LinkedIn*), purché tale utilizzo sia fatto nell'interesse dell'ente IUSTO e per lo sviluppo di collaborazioni o di partnership. Alcuni siti, come *LinkedIn*, permettono ai membri di segnalare colleghi e professionisti. Effettuare questo tipo di segnalazioni potrebbe essere considerato equivalente ad esprimere un parere a nome di IUSTO. Per questo motivo è necessario, ogni volta in cui si riceve una richiesta di segnalazione, agire con prudenza e con la consapevolezza di appartenere alla propria realtà organizzativa.
Per quanto riguarda i contatti tra i *Collaboratori* docenti e gli *Allievi*, devono essere utilizzati esclusivamente gli strumenti social e di messaggistica istituzionali (compresi quelli integrati nelle piattaforme di e-learning o learning management system). I *Collaboratori* non devono in nessun caso forzare gli *Allievi* ad aderire a loro gruppi social di tipo personale.
Qualora i *Collaboratori* e/o gli *Allievi* condividano liberamente l'appartenenza ad un gruppo social non creato o gestito da IUSTO sono tenuti a ricordare che esso non ha alcun carattere di ufficialità e che le comunicazioni ivi scambiate rientrano esclusivamente sotto la responsabilità personale dei loro autori, né possono essere ricondotte a IUSTO in alcun modo. Tutti sono pertanto invitati a valutare con ponderazione l'opportunità di aderire a tali gruppi.

### M. Rilevazione presenze

Per alcuni dei corsi erogati da IUSTO è attivo un sistema elettronico di rilevazione della presenza degli *Allievi* e dei *Collaboratori* docenti. L'attestazione della propria presenza avviene mediante badge personale assegnato al momento dell'iscrizione o della sottoscrizione del contratto.
I dati delle timbrature in entrata e in uscita raccolti dalle bollatrici poste all'ingresso di ogni aula vengono archiviati nei *Sistemi Informatici* in vista dell'attestazione dell'effettiva frequenza alle lezioni per gli *Allievi* e dello svolgimento dell'attività di docenza per i *Collaboratori* docenti.
La consultazione di tali dati da parte dei *Collaboratori* avviene secondo le linee guida interne sull'uso del registro elettronico. È possibile presentare istanza di modifica di eventuali errori o mancate timbrature utilizzando gli appositi strumenti di tracciamento delle richieste, come indicato nelle suddette linee guida, al sito *https://assistenza.ius.to/*.
In tutti i casi, gli *Utenti* non devono consentire a nessun altro di utilizzare il proprio badge, né utilizzare un badge altrui. La simulazione dell'identità di un altro *Utente* costituisce grave illecito e dà luogo a sanzioni disciplinari.

### N. Dati Personali

Tutti i dati personali in possesso di IUSTO devono essere trattati legittimamente e secondo etica. Qualsiasi dato personale, ai sensi del Regolamento UE 2016-679, deve essere trattato dagli *Utenti* in conformità alle vigenti leggi e a quanto previsto e stabilito dalle linee guida e dai documenti predisposti da IUSTO.
I *Collaboratori* devono essere consapevoli che:

- Tutti i dati personali raccolti, tenuti ed elaborati da IUSTO, sia usando documenti cartacei sia tramite computer, sono soggetti alla normativa sulla protezione dei dati. Essa descrive tipicamente le circostanze in cui i *Collaboratori* possono avere legittimo accesso, elaborare e rivelare dati personali. I *Collaboratori* di IUSTO devono attenersi a tali disposizioni, alle istruzioni del Titolare e, quando previsto, alle indicazioni contenute nel documento "Designazione del soggetto autorizzato incaricato al trattamento dei dati".
- Esiste un diritto dei soggetti a cui si riferiscono i dati di opporsi all'accesso, al trattamento ed alla comunicazione dei loro dati personali tenuti da IUSTO, ove tali soggetti ritengano che tale uso possa causare loro danni o pregiudizi rilevanti.

La politica aziendale di IUSTO per la tutela dei dati è descritta nei sopracitati documenti.

### O. Monitoraggio

IUSTO ha il diritto di effettuare monitoraggi periodici dei *Sistemi* e del loro uso per assicurarne la conformità al presente regolamento. Ogni monitoraggio sarà il più possibile automatizzato e rispetterà ogni disposizione relativa alla privacy.
In particolare:

- I diritti degli individui alla privacy per ciascuno dei propri dati personali tenuti nei *Sistemi* di IUSTO saranno rispettati. Tuttavia, IUSTO opera in base al presupposto che tutti i dati memorizzati sui supporti informatici di IUSTO sono di sua proprietà.
- Laddove necessario al fine di assicurare l'osservanza della legge e dei regolamenti aziendali, IUSTO si riserva il diritto di controllare – ed eventualmente limitare – gli accessi a siti e pagine web, fermo in ogni caso il rispetto dei principi di pertinenza e non eccedenza dei controlli.
- IUSTO ha il diritto di accedere alla posta elettronica aziendale, ma farà ciò soltanto se ci sia una ragione precisa per ritenere che le norme di condotta aziendali o la legislazione in vigore non siano state rispettate. Il contenuto della posta elettronica non sarà controllato, né divulgato, se non per ragioni di sicurezza e nei limiti delle norme di condotta aziendali e delle disposizioni di legge.
- La politica di IUSTO consiste nel non conservare i registri e gli output file associati ad un monitoraggio non necessario. Tali informazioni saranno soltanto conservate per un periodo non superiore a 12 mesi.

### P. Disabilitazione e cancellazione dell'account

In caso di cessazione del rapporto di lavoro, il *RSI* provvede a disabilitare/sospendere tutti gli account per l'accesso ai *Sistemi* del *Collaboratore* entro 7 giorni dal termine del rapporto di lavoro. Dopo 90 giorni dalla disabilitazione dell'account, lo stesso viene cancellato in via definitiva: pertanto anche l'home directory sul fileserver e i documenti personali ivi conservati non saranno più disponibili. Anche la casella mail aziendale verrà definitivamente disattivata al termine dei 90 giorni.
Per quanto riguarda gli *Allievi*, gli account vengono disattivati e cancellati 180 giorni dopo il termine del percorso di studi (discussione tesi e/o esame finale), eccezion fatta per la casella di posta elettronica istituzionale che rimane a loro disposizione finché essi non ne chiedano eventualmente la cancellazione. La segreteria studenti invia comunicazione della data di termine al *RSI*, che provvede a scadenziare la disabilitazione degli account.

### Q. Rispetto della legge

L'uso e la gestione di tutti i servizi informatici di IUSTO sono soggetti a tutte le leggi ed i regolamenti in materia, applicabili in Italia e nell'Unione Europea.
IUSTO può modificare il presente regolamento per ottemperare a nuove disposizioni di legge o per sopraggiunte necessità organizzative aziendali. IUSTO comunicherà ufficialmente tali modifiche a tutti gli *Utenti* dei *Sistemi*.

### R. Entrata in vigore e soggetto designato alla verifica

Il presente Regolamento entra in vigore dal 25 luglio 2019 e sostituisce integralmente il precedente regolamento emanato in data 1° marzo 2012 (prot. n. 20140906-09-183-SM). Tutti gli *Utenti* sono tenuti alla sua conoscenza, dedicandovi il tempo necessario, e alla sua osservanza.
Spetta al *RSI* vigilare, anche con verifiche a mezzo di controlli a sorpresa e/o a campione, sul corretto adempimento di quanto prescritto nel presente regolamento e dare esecuzione a quanto ivi previsto.