

Atto Direttoriale n. 13/2026

REGOLAMENTO PER LA SICUREZZA INFORMATICA E IL TRATTAMENTO DEI DATI

EMISSIONE DEL DOCUMENTO

	NOME	FUNZIONE
Redatto da	Raffaella Aglio Pomè Francesca	Responsabile Sistema di Gestione Addetta al Sistema di Gestione
Verificato da	Massimiliano De Maria	Responsabile Risorse Informatiche e Strumentali
Approvato da	Gabriele Cartasegna	Direttore

ELENCO DELLE EDIZIONI E REVISIONI

EDIZIONE	REVISIONE	DATA	OGGETTO DELLA REVISIONE
01	00	28/2/2019	Prima stesura
02	00	24/7/2019	Seconda Stesura
03	00	3/7/2024	Terza Stesura
04	00	15/09/2026	Quarta Stesura

SOMMARIO

PREMESSA	5
1. FINALITÀ	5
2. CAMPO DI APPLICAZIONE DEL REGOLAMENTO	5
3. ENTRATA IN VIGORE DEL REGOLAMENTO	6
4. NORMATIVA DI RIFERIMENTO	6
4.1 Normativa esterna	6
4.2 Normativa interna Capac	7
5. PRINCIPI E NORME DI CONDOTTA GENERALI	7
5.1 Riservatezza e protezione delle informazioni	7
5.2 Uso esclusivamente lavorativo	7
5.3 Tutela dei beni e delle risorse dell'Ente	7
5.4 Credenziali di autenticazione	7
5.5 Divieti generali	8
5.6 Conservazione dei log e controllo nel rispetto della privacy	8
6. REGOLE SPECIFICHE PER GLI STRUMENTI INFORMATICI	9
6.1 Personal computer	9
6.2 Rete aziendale e servizi cloud	10
6.3 Supporti Rimovibili	10
6.4 Posta elettronica	11
6.5 Disattivazione della casella di posta elettronica per cessazione del rapporto di lavoro	11
6.6 Metadati della posta elettronica	12
6.7 Navigazione in internet	12
6.8 Protezione antivirus	13
6.9 Social media	13
7. DISPOSIZIONI SPECIFICHE PER IL LAVORO AGILE	13
8. REGOLE SPECIFICHE PER GLI STRUMENTI NON ELETTRONICI	14
8.1 Documenti	14
8.2 Telefoni aziendali	15
8.3 Fax e fotocopiatrici	15
9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY	15
9.1 Controlli e informativa art. 4 Statuto dei Lavoratori	15
9.2 Responsabile della Protezione dei Dati (RPD/DPO)	16
9.3 Registro delle attività di Trattamento e Valutazione d'Impatto (DPIA)	16

9.4 Procedura di segnalazione delle violazioni dati personali (Data Breach)	16
10. NORME PER IL SISTEMA DI CONTROLLO DEGLI STRUMENTI E DEI SISTEMI INFORMATICI	17
10.1 Ruolo e poteri del RRIS (Amministratore di sistema)	17
10.2 Controlli gradualità	17
11. SANZIONI	18
12. AGGIORNAMENTO E REVISIONE	18
13. DISPOSIZIONI ULTERIORI	18
13.1 Trattamento di dati personali di studenti e corsisti	18
13.2 Videosorveglianza	18
13.3 Piattaforme digitali per la didattica e la formazione	19
13.4 Prevenzione del cyberbullismo e tutela dei minori in rete	19
13.5 Coordinamento con la sicurezza sul lavoro	19
13.6 Informazione sui sistemi automatizzati	19

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e il libero accesso a Internet ma anche le dinamiche sempre più elevate in termini di trattamento delle informazioni interne ed esterne, espongono la Fondazione CAPAC Politecnico del Commercio e del Turismo (di seguito denominato Ente) a responsabilità di tipo civile e penale connesse alla normativa sulla privacy (Reg. UE 679/2016 c.d. GDPR), ai delitti informatici e ai reati presupposto di cui al (D.Lgs. 231/2001), nonché a rischi per la sicurezza delle informazioni sensibili, della sua immagine pubblica e del know-how aziendale, quando queste informazioni di proprietà dell'Ente sono custodite nel sistema informatico. Il presente regolamento si coordina con il Modello di Organizzazione, Gestione e Controllo adottato dall'Ente ai sensi del D.Lgs. 231/2001.

1. FINALITÀ

L'Ente adotta il presente regolamento interno che contempla le principali norme comportamentali relative alla sicurezza dei dati e dei sistemi al fine di:

- prevenire comportamenti – anche inconsapevoli – che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e dei sistemi informatici, in linea con il principio di diligenza e correttezza richiamato nel Codice Etico vigente;
- integrare, senza sostituirla, l'informativa sul trattamento dei dati personali rilasciata dall'Ente applicabile per tipologia di rapporto (personale, collaboratori, ecc...) ai sensi dell'art. 13 del Regolamento (UE) 2016/679 (GDPR);
- disciplinare le modalità e i doveri che ciascuno/a deve osservare nell'utilizzo della strumentazione (telefoni, telefoni cellulari, computer portatili, tablet e smartphone, ecc.) che l'Ente ha messo loro a disposizione in ragione delle funzioni svolte.

2. CAMPO DI APPLICAZIONE DEL REGOLAMENTO

Il presente regolamento si applica a tutti coloro che, a qualsiasi titolo, utilizzano strumenti tecnologici dell'Ente o accedono alla sua rete informatica: dipendenti (senza distinzione di ruolo e/o livello), collaboratori/trici, lavoratori/trici somministrati/e, stagisti/e, prestatori/trici d'opera, consulenti o altri incaricati esterni.

Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi, anche mediante apposita clausola di rinvio che ne costituisca parte integrante del contenuto negoziale

Ai fini del presente Regolamento, per "utente" s'intende chiunque sia in possesso di credenziali di autenticazione rilasciate dall'Ente. Ai sensi del GDPR e del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, l'utente è designato quale "persona autorizzata al trattamento" ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, e riceve specifiche istruzioni operative dal Titolare del trattamento o dal Referente Privacy. Tale figura potrà essere designata anche come "Responsabile esterno del trattamento" od "Incaricato del trattamento", ai sensi del Codice Privacy.

Il Regolamento si applica integralmente anche alla prestazione lavorativa svolta in modalità di lavoro agile ai sensi della Legge n. 81/2017, con le specificazioni e le integrazioni previste dall'Accordo Quadro per la Disciplina del Lavoro Agile. L'utilizzo degli strumenti informatici dell'Ente da parte del/la lavoratore/trice agile al di fuori dei locali aziendali è soggetto/a alle medesime regole previste dal presente regolamento, nonché agli ulteriori obblighi di sicurezza e riservatezza derivanti dalla peculiarità del contesto extra-aziendale.

3. ENTRATA IN VIGORE DEL REGOLAMENTO

Il regolamento entra in vigore alla data della sua approvazione, sostituendo integralmente tutte le disposizioni precedentemente adottate in materia.

Copia del regolamento è consegnata a ciascun dipendente all'atto dell'assunzione, con raccolta di firma per ricevuta, ed è affissa, ai sensi dell'art. 4, comma 3°, della Legge n. 300/1970 (Statuto dei lavoratori) e degli obblighi di trasparenza di cui al D.Lgs. 104/2022. Per i collaboratori, il presente regolamento è richiamato nel contratto di collaborazione mediante apposita clausola di rinvio che ne costituisce parte integrante del contenuto negoziale, senza necessità di sottoscrizione separata del regolamento stesso. Il presente regolamento non sostituisce l'informativa sul trattamento dei dati personali rilasciata ai sensi dell'art. 13 del GDPR, che viene consegnata separatamente.

Il presente regolamento entra a far parte del Codice disciplinare.

4. NORMATIVA DI RIFERIMENTO

4.1 Normativa esterna

- Reg. (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)
- Garante per la protezione dei dati personali – “Linee guida del Garante per posta elettronica e internet – 10/3/2007– integrate e parzialmente sostituite, per la parte relativa ai metadati, dal successivo Provvedimento n. 364/2024.
- Garante per la protezione dei dati personali – Provvedimento del 27/11/2008 – “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” e ss.mm.ii., incluso il Provvedimento del 25/6/2009
- Legge del 20 maggio 1970, n. 300, “Statuto dei lavoratori”.
- Legge del 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300”.
- D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”, come modificato e integrato dal D.Lgs. 10 agosto 2018, n. 101.
- Garante per la protezione dei dati personali – Provvedimento n. 364 del 6/6/2024 – “Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”.
- D.Lgs. 27 giugno 2022, n. 104, recante “Attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell’Unione europea”.
- D.Lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679"
- D.Lgs. 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e ss.mm.ii.
- Legge del 29 maggio 2017, n. 71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"
- Legge del 22 maggio 2017, n. 81 “Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l’articolazione flessibile nei tempi e nei luoghi del lavoro subordinato”.

4.2 Normativa interna Capac

- Codice etico della Fondazione (vers.2 del 30/1/2024)
- Modello di Organizzazione, Gestione e Controllo della Fondazione (vers.1 del 21/3/2011)
- Organizzazione della Fondazione C.A.P.A.C. (vers.1 del 18/6/2014)
- Accordo Quadro per la Disciplina del Lavoro Agile della Fondazione C.A.P.A.C.
- Contratto integrativo di Ente 2025-2027

5. PRINCIPI E NORME DI CONDOTTA GENERALI

È obbligatorio osservare i principi e le norme di condotta definiti nel Codice Etico di Capac, in particolare:

- Trattamento delle informazioni e riservatezza
- Tutela della privacy del personale
- Dati e sistemi informatici che sono in relazione con la Pubblica Amministrazione
- Protezione e uso appropriato dei beni e delle risorse in generale
- Utilizzo degli strumenti informatici

5.1 Riservatezza e protezione delle informazioni

Le informazioni acquisite nello svolgimento delle attività lavorative:

- devono rimanere strettamente riservate e opportunamente protette;
- non possono essere utilizzate, comunicate o divulgate - all'interno o all'esterno dell'Ente - se non nel rispetto delle autorizzazioni ricevute, della normativa vigente e delle procedure interne;
- non possono essere utilizzate per scopi non connessi con l'esercizio della propria attività.

5.2 Uso esclusivamente lavorativo

Tutti gli strumenti informatici messi a disposizione dall'Ente (personal computer, telefoni, dispositivi mobili, posta elettronica, accesso a Internet, fax, fotocopiatrici) sono strumenti di lavoro. Il loro utilizzo è riservato esclusivamente allo svolgimento dell'attività lavorativa.

Qualsiasi utilizzo personale o non pertinente all'attività lavorativa è vietato, in quanto può contribuire a creare disservizi, costi aggiuntivi e minacce alla sicurezza delle informazioni. La risposta sanzionatoria alle violazioni del presente divieto è graduata secondo i principi di proporzionalità di cui al successivo capitolo 11 e alle previsioni del codice disciplinare.

5.3 Tutela dei beni e delle risorse dell'Ente

Ogni soggetto che opera per conto di CAPAC è tenuto a svolgere la propria attività con diligenza per tutelare i beni e le risorse dell'Ente nonché impedirne l'uso fraudolento o improprio.

5.4 Credenziali di autenticazione

L'utente si connette alla rete tramite autenticazione univoca personale. Le credenziali di autenticazione (user id e password) sono personali e riservate. L'utente è responsabile di custodirle con la massima diligenza e di preservarle dalla conoscenza di terzi. In particolare:

- le credenziali vengono assegnate dal Responsabile Risorse Informatiche e Strumentali (di seguito RRIS o Amministratore di sistema), previa indicazione della Direzione;

- consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata. La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri e/o simboli e/o punteggiatura, anche in combinazione fra loro, deve essere composta da almeno otto caratteri. Non si può riutilizzare una password già usata nelle ultime cinque modifiche;
- devono esser custodite dall'utente con la massima diligenza e preservate dalla conoscibilità di colleghi o soggetti esterni. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico;
- è assolutamente proibito accedere alla rete o ai programmi con credenziali altrui;
- l'accesso a sistemi esterni (piattaforme di enti finanziatori, PA) è autorizzato dalla Direzione; l'utente informa il RRIS per la registrazione nel database degli accessi esterni.

5.5 Divieti generali

È vietato a tutti gli/le utenti:

- accedere abusivamente o al di fuori delle autorizzazioni ricevute a sistemi informatici e telematici;
- diffondere o comunicare codici, password o altri mezzi di accesso a sistemi protetti;
- diffondere o comunque mettere a disposizione apparecchiature, dispositivi o programmi informatici diretti a danneggiare/interrompere il funzionamento di un sistema informatico/telematico o i dati/programmi in esso contenuti;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche;
- danneggiare, alterare o distruggere informazioni, dati, programmi o sistemi informatici/telematici;
- modificare la configurazione hardware/software del PC in dotazione senza autorizzazione del RRIS;
- installare software non ufficialmente fornito dall'Ente (inclusi freeware e shareware), per il rischio di virus e violazioni della normativa sul diritto d'autore;
- duplicare abusivamente programmi o contenuti di banche dati;
- mettere a disposizione in rete opere dell'ingegno protette;
- alterare il funzionamento di sistemi informatici interni o di enti esterni per conseguire un ingiusto profitto con danno altrui;
- salvare dati aziendali, documenti contenenti dati personali o informazioni riservate su servizi cloud personali o non autorizzati dall'Ente (es. account personali di Google Drive, Dropbox, OneDrive o analoghi).

L'Ente si riserva il diritto di adottare misure tecniche di sicurezza (es. firewall, filtri di navigazione, blacklist) che non abbiano come finalità il controllo a distanza dell'attività dei lavoratori. L'adozione di strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori è subordinata al rispetto delle procedure di cui all'art. 4, comma 1, della L. 300/1970 (accordo sindacale o autorizzazione dell'Ispettorato Nazionale del Lavoro).

5.6 Conservazione dei log e controllo nel rispetto della privacy

I log generati dai sistemi informatici dell'Ente (accessi, navigazione, posta elettronica) sono trattati nel rispetto della normativa sulla protezione dei dati personali e dell'art. 4 della Legge n. 300/1970 (Statuto dei lavoratori). In particolare:

- i log sono conservati in forma aggregata e anonima per finalità di sicurezza informatica e analisi del traffico; tale forma non consente l'identificazione diretta dell'utente;
- la conservazione in forma individuale (associata all'identità dell'utente) è ammessa esclusivamente in presenza di anomalie specifiche e per il tempo strettamente necessario alla loro risoluzione;
- in ogni caso, i log individuali non sono conservati per un periodo superiore a 21 (ventuno) giorni, salvo che la conservazione per un periodo più esteso sia necessaria per comprovate esigenze e sia stata preceduta dalle procedure di garanzia di cui all'art. 4, comma 1, Legge n. 300/1970 (accordo sindacale o autorizzazione dell'Ispettorato del lavoro);
- il controllo non è continuativo, costante o indiscriminato, né finalizzato al controllo dell'attività lavorativa del dipendente.

Le presenti disposizioni costituiscono adempimento degli obblighi informativi di cui all'art.4, comma 3, Legge 300/1970 e degli obblighi di trasparenza in materia di condizioni di lavoro di cui al D.Lgs. n.104/2022. L'informativa sul trattamento dei dati personali ai sensi dell'art.13 del GDPR è resa separatamente dal Titolare del trattamento.

6. REGOLE SPECIFICHE PER GLI STRUMENTI INFORMATICI

Le norme di questa sezione si aggiungono a quelle generali del capitolo 5 e disciplinano l'utilizzo degli strumenti informatici. Per quanto non espressamente previsto, si rinvia alle disposizioni del citato capitolo.

6.1 Personal computer

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato, perché può contribuire a creare disservizi, costi di manutenzione e soprattutto, minacce alla sicurezza delle informazioni.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione, come meglio descritto al precedente punto 5.4.

- Il personal computer deve essere custodito con cura, evitando ogni forma di danneggiamento;
- È vietato lasciare il computer incustodito e connesso alla rete senza attivare la schermata di blocco o di login, al fine di prevenire accessi non autorizzati da parte di terzi;
- In caso di temporanea assenza dalla postazione occorre attivare la schermata di blocco o di login. In caso di pause prolungate chiudere preventivamente documenti e applicazioni in lavorazione. Prima di lasciare gli uffici al termine dell'orario di lavoro o in caso di assenze prolungate, il PC deve essere spento;
- Non è consentita la modifica delle caratteristiche hardware e software impostate senza preventiva autorizzazione scritta del RRIS;
- Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal RRIS per conto dell'Ente, né installare autonomamente programmi informatici provenienti dall'esterno, anche nel caso in cui si tratti di software opportunamente licenziato, di software in prova (c.d. "shareware"), ovvero di software gratuito e liberamente scaricabile da Internet (c.d. "freeware"), sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti;
- L'inosservanza della presente disposizione espone l'Ente a gravi responsabilità civili; si evidenzia inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente;

- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il RRIS nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 6.8 del presente regolamento relativo alle procedure di protezione antivirus.

6.2 Rete aziendale e servizi cloud

Per l'accesso alla rete dell'Ente ciascun utente utilizza le credenziali personali assegnate dal RRIS (si rimanda al punto 5.4 per le relative regole).

- È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. La parola chiave d'ingresso alla rete ed ai programmi è segreta e va comunicata e gestita secondo le procedure impartite;
- Le cartelle utenti condivise sui server/NAS dell'Ente sono aree di condivisione di informazioni strettamente professionali per permettere collegamenti funzionali tra utenti che prestano servizio per l'Ente e non possono in alcun modo essere utilizzate per scopi diversi da quelli ai quali è destinata. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del RRIS;
- Le informazioni tecniche generate automaticamente dai sistemi di autenticazione al dominio (orari di accensione/spegnimento, log di accesso a risorse di rete) costituiscono dati raccolti attraverso gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa ai sensi dell'art. 4, comma 2, Legge n. 300/1970, e possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, essendo stata fornita adeguata informazione ai lavoratori ai sensi del precedente punto 5.6. Tali informazioni non sono utilizzate per effettuare un controllo sistematico, costante o indiscriminato dell'attività lavorativa;
- Con regolare periodicità (almeno ogni sei mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili ed evitando l'archiviazione ridondante;
- L'accesso da remoto alla rete dell'Ente è possibile solo agli utenti abilitati, tramite le credenziali o il software VPN predisposto dal RRIS;
- L'utilizzo delle reti WiFi aziendali è limitato agli utenti autorizzati con credenziali assegnate dal RRIS;
- L'utilizzo di servizi informatici erogati in modalità cloud o as-a-service (posta elettronica, archiviazione documenti, piattaforme di collaborazione) è consentito esclusivamente per i servizi preventivamente autorizzati e configurati dal RRIS. L'utente non è autorizzato a sottoscrivere, attivare o utilizzare servizi cloud diversi da quelli ufficialmente predisposti dall'Ente. È vietato il salvataggio di dati aziendali, documenti contenenti dati personali o informazioni riservate su servizi cloud personali o non autorizzati dall'Ente (quali, a titolo esemplificativo, account personali di Google Drive, Dropbox, OneDrive o servizi analoghi).

6.3 Supporti rimovibili

- I supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela, e adeguatamente custoditi in armadi chiusi, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato;
- È vietato l'utilizzo di supporti rimovibili personali;
- Per la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, contattare il RRIS e seguire le istruzioni da questo impartite;
- In caso di restituzione di dispositivi aziendali (PC portatili, tablet ecc.) sui quali possano venir salvati documenti, dati ed altro materiale, provvedere al salvataggio in opportuni supporti esterni

del necessario o alla sua rimozione effettiva prima della riconsegna del dispositivo, concordando ogni azione con il RRIS.

6.4 Posta elettronica

- La casella di posta elettronica assegnata all'utente deve essere consultata con frequenza giornaliera, salvo casi di assenza dal lavoro;
- È obbligatorio mantenere la casella di posta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
- I messaggi devono contenere un avvertimento standardizzato sulla natura aziendale e non personale;
- È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- In caso di assenza programmata (es. ferie, attività di lavoro fuori sede) l'utente chiede al RRIS l'attivazione del messaggio di risposta automatica contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura;
- In caso di assenza non programmata (es. per malattia) qualora l'utente non possa attivare autonomamente la risposta automatica tramite webmail entro due giorni, verrà attivata dal RRIS;
- È vietato utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
 - l'invio o la memorizzazione di messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscono comunque condotta illecita;
 - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
 - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
 - partecipare a catene telematiche (o di Sant'Antonio).
- È obbligatorio prestare la massima attenzione nell'aprire i file allegati a messaggi di posta elettronica e non eseguire download di file eseguibili (programmi di installazione) o documenti da siti Web o server FTP non conosciuti;
- In caso di assenza o indisponibilità del titolare della casella, l'accesso ai contenuti della posta elettronica da parte del RRIS è consentito esclusivamente per comprovate e documentate esigenze di continuità operativa, con le seguenti garanzie: (i) preventiva comunicazione al lavoratore, ove possibile; (ii) accesso limitato ai messaggi strettamente pertinenti all'esigenza operativa; (iii) documentazione di ogni accesso in apposito registro conservato a cura del RRIS. In conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni, ogni accesso del RRIS alle caselle di posta elettronica, anche al di fuori dei casi di assenza o indisponibilità del titolare e per qualsiasi finalità (manutenzione, sicurezza, verifiche tecniche), è parimenti documentato nel medesimo registro, con l'indicazione della data, dell'ora, della casella di accesso e della motivazione;
- L'assegnazione e il ritiro della casella di posta elettronica sono disposti dalla Direzione in base alle esigenze organizzative e funzionali dell'Ente.

6.5 Disattivazione della casella di posta elettronica per cessazione del rapporto di lavoro

- In previsione della cessazione del rapporto di lavoro, il/la dipendente è tenuto/a ad eliminare dai propri archivi informatici i messaggi e i documenti di natura non pertinente all'attività dell'Ente. Entro un congruo termine comunicato dalla Direzione e, comunque, prima dell'effettiva

cessazione, al/alla lavoratore/trice è offerta la possibilità di rimuovere dalla casella di posta e dalle cartelle personali eventuali messaggi e documenti di natura strettamente personale. La restante corrispondenza e documentazione inerente all'attività lavorativa è conservata dall'Ente come documentazione lavorativa;

- La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro. Per le funzioni apicali la casella di posta e l'account rimarranno attive per un periodo congruo, comunque, non superiore ai 3 mesi per esigenze di coordinamento con la risorsa che sostituisce l'ex dipendente;
- Alla cessazione del rapporto di lavoro di funzioni non apicali ovvero decorso il periodo previsto per le funzioni apicali di cui al precedente punto:
 - a. è attivato un sistema di risposta automatica che informa i mittenti della disattivazione dell'account e fornisce un indirizzo alternativo di contatto;
 - b. l'accesso ai contenuti della casella è consentito al RRIS esclusivamente per finalità di continuità operativa, con modalità proporzionate e nel rispetto della normativa sulla protezione dei dati personali;
 - c. decorso il termine di cui al presente comma, l'account e i relativi contenuti sono definitivamente cancellati.

6.6 Metadati della posta elettronica

I metadati generati automaticamente dai sistemi di posta elettronica (c.d. log di trasporto: indirizzi e-mail mittente/destinatario, indirizzi IP dei server, orari di invio/ricezione, dimensione del messaggio e degli allegati) sono conservati per un periodo non superiore a 21 (ventuno) giorni dalla data di registrazione, in conformità al Documento di indirizzo del Garante per la protezione dei dati personali del 6/6/2024 (Prov. n. 364).

Tale periodo di conservazione è funzionale ad assicurare il corretto funzionamento e la regolare manutenzione del sistema di posta elettronica, nonché la sicurezza informatica. Decorso tale termine, i metadati sono cancellati automaticamente ovvero resi anonimi in modo irreversibile.

La conservazione oltre ai 21 giorni, ove necessaria per comprovate e documentate esigenze organizzative, produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale, è subordinata al previo espletamento delle procedure di garanzia previste dall'art. 4, comma 1, della Legge n. 300/1970 (accordo con le rappresentanze sindacali ovvero autorizzazione dell'Ispettorato del lavoro).

Le presenti disposizioni non riguardano i contenuti dei messaggi, né le informazioni tecniche che ne fanno parte integrante, che restano nella disponibilità dell'utente assegnatario/a della casella di posta.

6.7 Navigazione in internet

- La navigazione è consentita esclusivamente per finalità lavorative;
- l'Ente adotta sistemi di blocco o filtro automatico (black list) per prevenire l'accesso a siti non pertinenti all'attività lavorativa. Tali sistemi sono configurati in modo da non generare log individuali associati all'identità dell'utente, salvo il caso di accesso a siti in black list, i cui log sono conservati in forma anonimizzata per finalità di sicurezza informatica. In presenza di specifiche anomalie, i log possono essere associati all'utente nei limiti e con le garanzie di cui al punto 5.6;
- I log della navigazione sono trattati secondo quanto previsto al punto 5.6. I log relativi a tentativi di accesso a siti in black list sono conservati in forma anonimizzata, salvo il caso di anomalie specifiche;

A titolo esemplificativo, è vietato utilizzare Internet per:

- a. upload o download di software freeware/shareware o documenti (filmati, musica) non attinenti all'attività lavorativa;
- b. transazioni finanziarie (remote banking, acquisti on-line e simili);
- c. registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- d. partecipazione a forum non professionali, chat line non autorizzate, bacheche elettroniche, guest book;
- e. accesso a caselle webmail personali.

6.8 Protezione antivirus

Il sistema informatico dell'Ente è protetto da software antivirus aggiornato quotidianamente in automatico. Ogni utente deve:

- tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo;
- nel caso il software antivirus rilevi la presenza di un virus, segnalare immediatamente l'anomalia al RRIS e nei casi di livello molto grave indicati dal software, sospendere ogni elaborazione in corso senza spegnere il computer;
- verificare con il programma antivirus qualsiasi dispositivo magnetico di provenienza esterna prima del suo utilizzo.

6.9 Social media

- L'utilizzo a fini promozionali e commerciali dei social media (Facebook, Twitter, LinkedIn, YouTube, blog, forum) è gestito esclusivamente dall'Ente tramite personale appositamente incaricato; sono escluse iniziative individuali;
- L'utilizzo degli strumenti informatici aziendali per accedere a piattaforme di social media per fini non lavorativi è vietato durante l'orario di lavoro. L'utilizzo di dispositivi personali per accedere ai social media è consentito esclusivamente durante le pause e non deve interferire con lo svolgimento dell'attività lavorativa;
- La condivisione di contenuti sui social media deve rispettare la riservatezza delle informazioni dell'Ente (es. informazioni finanziarie, commerciali, piani didattici, dati su clienti, fornitori, partner, ecc.) e i diritti di proprietà industriale e d'autore sia di terzi che dell'Ente. L'utente non può utilizzare marchi o segni distintivi dell'Ente, né pubblicare disegni, modelli o contenuti connessi a tali diritti;
- L'utente garantisce la tutela della privacy delle persone: non può comunicare o diffondere dati personali (dati anagrafici, immagini, video, audio) di colleghi o collaboratori senza il loro preventivo consenso, né pubblicare contenuti registrati nei luoghi di lavoro senza il consenso del Referente Privacy;
- L'utente risponde personalmente dei propri comportamenti e deve astenersi da condotte penalmente o civilmente rilevanti (atti ingiuriosi, diffamatori, discriminatori o molestie) nei confronti di terzi, dell'Ente, dei colleghi, dei clienti e dei fornitori.

7. DISPOSIZIONI SPECIFICHE PER IL LAVORO AGILE

Le disposizioni del presente regolamento si applicano integralmente alla prestazione svolta in modalità di lavoro agile ai sensi della Legge n. 81/2017. Il lavoratore agile è tenuto, anche al di fuori dei locali aziendali, al

rispetto di tutte le prescrizioni del presente regolamento, con le specificazioni di cui ai commi seguenti e le ulteriori disposizioni previste dall'Accordo Quadro per la Disciplina del Lavoro Agile.

In aggiunta agli obblighi di cui ai precedenti paragrafi, il lavoratore che svolge la prestazione in modalità agile è tenuto a:

- a. utilizzare esclusivamente connessioni di rete sicure e protette da credenziali. È vietato l'utilizzo di reti WiFi pubbliche non protette (quali reti aperte di locali pubblici, aeroporti, stazioni) per l'accesso a dati, informazioni e sistemi dell'Ente, salvo l'utilizzo della connessione VPN aziendale;
- b. posizionare lo schermo del dispositivo in modo da impedire la visualizzazione delle informazioni da parte di soggetti non autorizzati, ivi compresi familiari e conviventi;
- c. non salvare dati aziendali, documenti contenenti dati personali o informazioni riservate su dispositivi personali, supporti rimovibili personali o servizi cloud non aziendali;
- d. non consentire a terzi, inclusi familiari e conviventi, l'accesso agli strumenti aziendali o la visualizzazione di informazioni, documenti e dati trattati;
- e. segnalare immediatamente al RRIS e alla Direzione qualsiasi anomalia, tentativo di accesso non autorizzato, sospetta infezione da virus/malware o altra violazione della sicurezza informatica;
- f. segnalare immediatamente al Referente Privacy e alla Direzione qualsiasi violazione o sospetta violazione della sicurezza dei dati personali (c.d. data breach);
- g. in caso di guasto o indisponibilità della connessione internet presso il luogo esterno, comunicarlo tempestivamente al proprio responsabile gerarchico e al RRIS;
- h. i documenti contenenti dati personali stampati presso il luogo di lavoro esterno, previa autorizzazione del proprio responsabile gerarchico, devono essere custoditi con la massima diligenza e distrutti una volta cessata l'esigenza lavorativa.

L'utilizzo di dispositivi personali del lavoratore (c.d. BYOD) per lo svolgimento della prestazione in modalità agile è consentito esclusivamente nei limiti e con le condizioni stabiliti dall'art. 9 dell'Accordo Quadro per la Disciplina del Lavoro Agile.

Il lavoratore agile è tenuto al rispetto del diritto alla disconnessione e dei limiti orari previsti dall'Accordo Quadro e dall'accordo individuale di lavoro agile. Lo svolgimento dell'attività lavorativa nelle ore notturne (dalle 22:00 alle 5:00) è vietato, salvo diversa previsione dell'accordo individuale e comunque nel rispetto dei limiti inderogabili di orario di lavoro previsti dal D.Lgs. 66/2003 e dal CCNL applicabile.

8. REGOLE SPECIFICHE PER GLI STRUMENTI NON ELETTRONICI

Questo capitolo riguarda il trattamento delle informazioni gestite in formato cartaceo e con utilizzo dei telefoni, fax e fotocopiatrici aziendali.

8.1 Documenti

- Non devono essere lasciati in vista documenti contenenti informazioni o dati personali riservate in presenza di personale esterno o comunque non autorizzato al trattamento;
- Al termine dell'orario di lavoro i documenti riservati devono essere riposti in luogo adeguatamente protetto;
- Non riutilizzare a scopo di riciclo documenti cartacei contenenti informazioni riservate e dati personali;

- I documenti cartacei riservati destinati all'eliminazione devono essere efficacemente distrutti;
- I luoghi di lavoro con documenti riservati e dati personali non devono essere accessibili a persone non autorizzate senza il presidio di personale autorizzato al trattamento.

8.2 Telefoni aziendali

- Il telefono aziendale (fisso e cellulare) è uno strumento di lavoro riservato all'attività lavorativa; non sono consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa;
- Non fornire telefonicamente informazioni riservate a persone non autorizzate a riceverle;
- Le telefonate personali sono consentite solo in caso di comprovata necessità ed urgenza, tramite il telefono fisso aziendale;
- Il cellulare aziendale segue le stesse regole del telefono fisso; in particolare, è vietato l'utilizzo per inviare o ricevere SMS o MMS personali. L'eventuale uso promiscuo (anche personale) è possibile soltanto con preventiva autorizzazione scritta della Direzione;
- L'assegnatario/a del cellulare aziendale è responsabile del suo utilizzo e della sua custodia.

8.3 Fax e fotocopiatrici

- È vietato l'utilizzo dei fax e delle fotocopiatrici aziendali per fini personali, salva diversa esplicita autorizzazione da parte della Direzione;
- È obbligo rimuovere i documenti originali dai fax e dalle fotocopiatrici dopo l'utilizzo.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

9.1 Controlli e informativa art. 4 Statuto dei Lavoratori

- 9.1.1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Nell'ambito dello svolgimento delle funzioni all'interno della Struttura Organizzativa dell'Ente, il/la dipendente è assoggettato/a alle disposizioni dello stesso e del Referente Privacy. In particolare, venendo necessariamente a conoscenza dei contenuti di Dati Personali trattati sia su base cartacee che tramite strumenti informatici e svolgendo operazioni di trattamento, per poter espletare correttamente la propria mansione lavorativa deve garantire il rispetto e la giusta applicazione delle procedure e delle istruzioni implementate dal Titolare in ambito GDPR, impartite tramite apposita nomina ad Autorizzato al trattamento dei dati personali.
- 9.1.2. Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970, conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data adeguata informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico dell'Ente ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 9.2), fermo restando il rispetto della normativa in materia di protezione dei dati personali. Le disposizioni del presente comma si applicano integralmente anche agli strumenti tecnologici utilizzati per lo svolgimento della prestazione in modalità di lavoro agile. Il presente regolamento, unitamente all'Accordo Quadro per la Disciplina del Lavoro Agile e all'accordo individuale, costituisce adempimento degli obblighi informativi di cui all'art. 4, comma

3, della Legge n. 300/1970 e degli obblighi di trasparenza in materia di condizioni di lavoro di cui al D.lgs. n. 104/2022 e comunque nel rispetto dei limiti inderogabili di orario di lavoro previsti dal D.lgs. 66/2003 e dal CCNL applicabile.

- 9.1.3. Non sono installati o configurati sui sistemi informatici in uso agli/alle utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei/delle lavoratori/trici; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per altre finalità, es. esigenze organizzative, di sicurezza del lavoro e/o di tutela del patrimonio, l'Ente provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n. 300/1970, dandone anche opportuna informazione agli utenti stessi.

9.2 Responsabile della Protezione dei Dati (RPD/DPO)

La Fondazione ha designato il Responsabile della Protezione dei Dati (RPD/DPO) ai sensi dell'art. 37 del Regolamento (UE) 2016/679. Il DPO è raggiungibile all'indirizzo e-mail [dpo@capac.it]. Chiunque ritenga che il trattamento dei propri dati personali violi le disposizioni del Regolamento può rivolgersi al DPO prima di presentare un reclamo al Garante per la protezione dei dati personali. Il DPO è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, ai sensi dell'art. 38 del GDPR.

9.3 Registro delle Attività di Trattamento e Valutazione d'Impatto (DPIA)

L'Ente mantiene e aggiorna il Registro delle Attività di Trattamento ai sensi dell'art. 30 del GDPR. Tutti i trattamenti di dati personali effettuati nell'ambito delle attività disciplinate dal presente regolamento sono iscritti nel Registro.

Per i trattamenti che comportano rischi elevati per i diritti e le libertà delle persone fisiche, l'Ente effettua preventivamente una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del GDPR, consultando il DPO. I risultati della DPIA sono documentati e conservati nel Registro dei Trattamenti.

9.4 Procedura di segnalazione delle violazioni dati personali (Data Breach)

Ogni utente che venga a conoscenza di una violazione o di una sospetta violazione della sicurezza dei dati personali (c.d. data breach) è tenuto a segnalarla immediatamente, e comunque senza ingiustificato ritardo, al Referente Privacy e alla Direzione.

Costituiscono esempi di violazioni dei dati personali:

- smarrimento o il furto di dispositivi contenenti dati personali;
- accesso non autorizzato a sistemi, archivi o caselle di posta elettronica;
- comunicazione o diffusione accidentale di dati personali a soggetti non autorizzati;
- infezione da virus/malware che comprometta la riservatezza, l'integrità o la disponibilità dei dati;
- qualsiasi malfunzionamento degli strumenti che comprometta la sicurezza dei dati.

La segnalazione deve contenere, ove possibile, la natura della violazione, le categorie e il numero approssimativo di interessati coinvolti, le probabili conseguenze della violazione e le misure adottate o proposte.

La Direzione, con il supporto del Referente Privacy e del RRIS, valuta la violazione e, ove ne ricorrano i presupposti ai sensi dell'art. 33 del GDPR, provvede alla notifica al Garante entro 72 ore dal momento in cui ne è venuta a conoscenza. Ove la violazione sia suscettibile di presentare un rischio elevato per i diritti e le

libertà delle persone fisiche, la comunicazione è effettuata anche agli interessati, ai sensi dell'art. 34 del GDPR.

Il RRIS tiene un registro delle violazioni dei dati personali ai sensi dell'art. 33, paragrafo 5, del GDPR, nel quale sono documentate le circostanze della violazione, le relative conseguenze e i provvedimenti adottati per porvi rimedio.

10. NORME PER IL SISTEMA DI CONTROLLO DEGLI STRUMENTI E DEI SISTEMI INFORMATICI

10.1 Ruolo e poteri del RRIS (Amministratore di Sistema)

È facoltà della Direzione accedere tramite il RRIS nel rispetto della normativa privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa.

La facoltà di accesso si estende ai dispositivi utilizzati dal personale in modalità agile, nei medesimi limiti e con le medesime finalità. In caso di accesso a dispositivi utilizzati al di fuori dei locali aziendali, il RRIS ne dà preventiva comunicazione al lavoratore, ove ciò non pregiudichi la tempestività e l'efficacia dell'intervento.

In particolare, il RRIS:

- è autorizzato a compiere interventi nel sistema informatico aziendale in qualità di Amministratore di sistema, diretti a garantire la funzionalità e la sicurezza del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.) o per finalità di controllo e programmazione dei costi aziendali;
- può collegarsi e visualizzare in remoto il desktop delle singole postazioni PC, al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data all'utente comunicazione della necessità dell'intervento stesso;
- può procedere in qualunque momento alla rimozione di ogni file o applicazione, che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete;
- può effettuare controlli graduali;
- è tenuto a segnalare alla Direzione ogni violazione del Codice Etico e del presente regolamento.

10.2 Controlli graduali

- In caso di anomalie, il RRIS effettua controlli anonimi che si concluderanno con avvisi generalizzati, nei quali si evidenzierà l'utilizzo irregolare degli strumenti dell'Ente e con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere compiuti solo a fronte di fondato sospetto circa la commissione di comportamenti illeciti o in violazione del presente regolamento, e in ogni caso in presenza di successive ulteriori anomalie.
- Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti

dagli utenti abilitati alla navigazione esterna. L'accesso ai contenuti della casella di posta elettronica per finalità di controllo disciplinare è soggetto alle garanzie procedurali di cui al punto 6.4.

- La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'ente, si applica anche in caso di assenza prolungata od impedimento dell'utente.
- In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

11. SANZIONI

Il mancato rispetto o la violazione delle disposizioni del presente Regolamento è perseguibile nei confronti:

- del personale dipendente secondo le procedure e con le sanzioni previste dal codice disciplinare di cui al CCNL della Formazione Professionale e all'art. 7 della Legge n. 300/1970. Resta ferma l'azione di responsabilità per il risarcimento dei danni eventualmente cagionati all'Ente. La violazione delle disposizioni in materia di protezione dei dati personali è altresì perseguibile ai sensi del Regolamento (UE) 2016/679 e del D.lgs. 196/2003;
- dei/delle collaboratori/trici, consulenti ed incaricati esterni, verificata la gravità della violazione contestata, con la risoluzione dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

12. AGGIORNAMENTO E REVISIONE

Tutti gli/le utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto periodicamente a revisione. Le revisioni sono portate a conoscenza di tutti gli utenti mediante i canali di comunicazione interna e, ove riguardino modifiche sostanziali, sono oggetto di nuova consegna con raccolta di firma per ricevuta.

13. DISPOSIZIONI ULTERIORI

13.1 Trattamento dei dati personali di studenti e corsisti

I dati personali degli/delle studenti/esse, dei/delle corsisti/e e dei loro familiari sono trattati dall'Ente esclusivamente per le finalità istituzionali connesse all'erogazione dei servizi formativi, nel rispetto del GDPR, del D.Lgs. 196/2003 e delle indicazioni del Garante per la protezione dei dati personali. I dati di soggetti minorenni sono trattati con misure di protezione rafforzate, in conformità al considerando art. 38 del GDPR e all'art. 8 del medesimo Regolamento. Il personale docente e amministrativo che viene a conoscenza di dati relativi a studenti o corsisti è tenuto alla massima riservatezza e non può comunicarli a soggetti non autorizzati, né inserirli in circolari o comunicazioni collettive non rivolte a specifici destinatari.

13.2 Videosorveglianza

Gli impianti di videosorveglianza eventualmente installati presso le sedi della Fondazione sono attivati nel rispetto dell'art. 4, comma 1, della Legge n. 300/1970 (previa stipula di accordo con le rappresentanze sindacali o autorizzazione dell'Ispettorato Nazionale del Lavoro) e delle prescrizioni del Garante per la protezione dei dati personali. Le immagini sono conservate per un periodo non superiore a 48 ore, salvo esigenze specifiche documentate (giorni festivi, chiusura dell'Ente, indagini delle autorità), dopodiché sono cancellate automaticamente. In prossimità di ogni sistema di videosorveglianza è apposto idoneo cartello informativo ai sensi dell'art. 13 del GDPR.

13.3 Piattaforme digitali per la didattica e la formazione

L'utilizzo delle piattaforme digitali per l'erogazione delle attività formative (es. sistemi LMS, piattaforme di videoconferenza, ambienti collaborativi) è consentito esclusivamente per le piattaforme preventivamente autorizzate e configurate dall'Ente, che ne valuta la conformità al GDPR e agli standard di sicurezza. È vietata la videoregistrazione delle sessioni formative che manifesti le dinamiche di classe senza il previo consenso informato di tutti i partecipanti, acquisito nelle forme previste dalla normativa vigente. Non è ammessa la diffusione, anche parziale, di contenuti delle sessioni formative su piattaforme non autorizzate o canali social.

13.4 Prevenzione del cyberbullismo e tutela dei/delle minori in rete

L'Ente adotta misure organizzative e formative per prevenire e contrastare fenomeni di cyberbullismo all'interno della propria comunità formativa, in conformità alla Legge del 29 maggio 2017, n. 71. È designato un referente per il cyberbullismo tra il personale della Fondazione. Ogni episodio riconducibile a forme di cyberbullismo deve essere segnalato immediatamente al Referente e alla Direzione, che valutano le misure da adottare, inclusa la segnalazione alle autorità competenti.

13.5 Coordinamento con la sicurezza sul lavoro

Le disposizioni del presente regolamento si coordinano con gli obblighi organizzativi e documentali in materia di salute e sicurezza nei luoghi di lavoro di cui al D.lgs. 9 aprile 2008, n. 81 e ss.mm.ii., con particolare riferimento alla sicurezza delle attrezzature munite di videoterminali e agli obblighi di informazione e formazione dei lavoratori.

13.6 Informazione sui sistemi automatizzati

Ai sensi dell'art. 1-bis del D.Lgs. del 26 maggio 1997, n. 152, come modificato dal D.L. 4 maggio 2023, n. 48 (convertito con Legge 3 luglio 2023, n. 85), l'Ente informa il lavoratore dell'eventuale utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati incidenti sul rapporto di lavoro, fermo restando quanto disposto dall'art. 4 della Legge n. 300/1970. Resta escluso qualsiasi trattamento automatizzato finalizzato alla profilazione del lavoratore o alla valutazione sistematica delle sue prestazioni, se non nei limiti e con le garanzie previste dalla legge.

Milano, 15 settembre 2026

Il Direttore

Gabriele Cartasegna

