Protocollo 0022377/2026 del 16/10/2026

ISTITUTO COMPRENSIVO STATALE "CARLO RIDOLFI"
Viale della Repubblica, 6 - 36045 LONIGO (VI)
C.F. 80016190243 - Cod.Min. VIIC818008
Tel. 0444 830244 - 0444 830245
e-mail: VIIC818008@ISTRUZIONE.IT - P.E.C.: VIIC818008@PEC.ISTRUZIONE.IT
www.icridolfi.edu.it

POLICY

GESTIONE DELLA POSTA ELETTRONICA

COD. C.09
VERS. 02 DEL 02.2026

CONTIENE:

1. POLICY

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE
02	01.02.2026	AGGIORNAMENTO AI NUOVI ORIENTAMENTI GIURISPRUDENZIALI

Copyright 2022
EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale

ISTITUTO COMPRENSIVO STATALE "CARLO RIDOLFI"
Viale della Repubblica, 6 - 36045 LONIGO (VI)
C.F. 80016190243 - Cod.Min. VIIC818008
Tel. 0444 830244 - 0444 830245
e-mail: VIIC818008@ISTRUZIONE.IT - P.E.C.: VIIC818008@PEC.ISTRUZIONE.IT
www.icridolfi.edu.it

PREMESSA

Secondo orientamento costante del Garante Privacy, compete ai datori di lavoro, e quindi ai Dirigenti Scolastici, assicurare la funzionalità e il corretto impiego della posta elettronica istituzionale da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali.
Non solo, in base al GDPR, spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità. In questo contesto è utile ricordare che il corretto utilizzo dei sistemi di posta elettronica è necessità prevista da un lato a tutela dell'utenza (ad esempio degli studenti) e dall'altro a tutela dei diritti del lavoratore.
L'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza.

CREAZIONE ACCOUNT

In occasione dell'avvio del rapporto di lavoro e/o di collaborazione, saranno fornite al collaboratore delle credenziali per entrare nell'account di posta elettronica creato appositamente utilizzando i dati anagrafici dello stesso (solitamente nome e cognome).
A tal riguardo, ove possibile, sarebbe preferibile minimizzare l'impatto di tale trattamento, ad esempio, sostituendo il cognome per esteso ad una sola iniziale oppure ad un codice. Creato l'account, nel rispetto di quanto sopra, sarà necessario fornire delle chiavi di ingresso al collaboratore. I collaboratori devono essere espressamente invitati a modificare le credenziali di accesso, e in particolare la password, contestualmente al primo log in, in modo da evitare possibili accessi abusivi. Si precisa che, in taluni casi, l'indirizzo mail potrebbe essere condiviso (es: segreteria@lamiascuola.it). In questo caso il personale non potrà che attendersi un più basso livello di riservatezza sulle comunicazioni ivi transitanti, in quanto le stesse saranno per loro natura lette da tutti coloro che sono autorizzati ad utilizzare tale account di funzione.

TUTELA DEL LAVORATORE

Il luogo di lavoro deve necessariamente essere organizzato in modo da garantire la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati. Per questo motivo, salvo rare eccezioni, è da ritenersi assolutamente vietato il controllo dei lavoratori e dei loro strumenti di lavoro.
In ogni caso, a prescindere dal controllo, il lavoratore è comunque tenuto ad osservare le seguenti regole nella navigazione e nell'utilizzo della posta elettronica istituzionale:

1. il download di file (testo, video, foto, audio…) è possibile solo se l'origine degli stessi è di carattere istituzionale (Ministero, Dirigente Scolastico, altre PA) non essendo in alcun modo consentito il download proveniente da altri siti, salvo espressa autorizzazione del DPO;
2. anche nel caso in cui il file fosse stato apparentemente inviato da un mittente attendibile, prima di procedere con il download è richiesto di verificare con assoluta perizia il mittente al fine di confermare l'origine autentica del messaggio di posta elettronica;
3. non è in alcun modo consentito l'utilizzo dei servizi di posta elettronica istituzionali per motivi personali quali, ad esempio: prenotazioni di viaggi, acquisti on line, creazione di account sui social ecc. ecc. Allo stesso modo è fatto divieto di utilizzo per motivi personali anche dei servizi scolastici quali: server, sistemi di archiviazione in cloud, ogni tipo di sistema in dotazione alla scuola;

Copyright 2022
EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale

4. in caso di allontanamento dalla postazione è necessario disconnettersi dai servizi di posta elettronica in uso o, quantomeno, inserire uno *screensaver* che impedisca l'accesso al device a coloro che non siano in possesso della apposita password;
5. è possibile che i servizi in dotazione alla scuola registrino file di log capaci di determinare i momenti di accesso o di disconnessione dagli stessi. Tali file non verranno dall'Istituzione controllati in alcun modo salvo il verificarsi di circostanza espressamente previste per legge (es: in caso di data breach per verificare il numero di soggetti che hanno visualizzato una certa pagina in un determinato momento).

CASI DI ASSENZA

È necessario che il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad esempio per ferie), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.
É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica a soggetti terzi. In caso di eventuali assenze non programmate (ad esempio per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando l´assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad esempio l´amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l´attivazione di un analogo accorgimento, avvertendo gli interessati.
In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, è opportuno che l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile. Anche per questo, i messaggi di posta elettronica dovrebbero contenere un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

CONTROLLI

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Solo in presenza di un fondato e specifico sospetto di illecito, e nel rispetto dei presupposti e dei limiti individuati dalla normativa vigente e dalla giurisprudenza in materia di controlli difensivi del datore di lavoro, potrà essere autorizzato l'accesso alla casella di posta elettronica istituzionale assegnata al dipendente o collaboratore, esclusivamente al fine di accertare eventuali condotte illecite.

Copyright 2022
EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale

Tale accesso deve essere limitato allo stretto necessario, circoscritto ai messaggi, alle comunicazioni o ai metadati pertinenti rispetto ai fatti oggetto di verifica, ed effettuato in modo da ridurre al minimo l'incidenza sui diritti e sulle libertà dell'interessato.
Anche in tale ipotesi, il Dirigente incaricherà un **soggetto specificamente designato**, anche interno all'Istituzione, adeguatamente istruito e vincolato alla riservatezza, con il compito di:

- limitare l'accesso alle sole comunicazioni strettamente pertinenti all'accertamento dell'illecito;
- **epurare e non utilizzare** ogni informazione superflua, non rilevante o attinente alla sfera personale del dipendente o collaboratore;
- garantire la **tracciabilità delle operazioni effettuate**, nonché il rispetto delle misure di sicurezza tecniche e organizzative previste.

In ogni caso, il trattamento dei dati personali effettuato nell'ambito delle attività sopra descritte avviene nel rispetto della normativa in materia di protezione dei dati personali e della disciplina sui controlli a distanza dei lavoratori, assicurando informativa preventiva ai lavoratori, nonché adeguate garanzie a tutela dei diritti e delle libertà degli interessati.

DISATTIVAZIONE ACCOUNT

In base all'orientamento del Garante Privacy è errato mantenere attiva la posta elettronica dell'ex dipendente, ad esempio, impostando un messaggio di inoltro automatico verso altro indirizzo di altro dipendente. Questo difatti, violerebbe le aspettative di riservatezza tanto dell'ex dipendente quanto del mittente il quale, credendo di parlare con il soggetto "Tizio" potrebbe rivelare informazioni riservate che magari non vorrebbe comunicare a "Caio". Per questo motivo, dopo la cessazione del rapporto, è necessario disattivare, come modalità di gestione regolare, l'account di posta elettronica dell'ex dipendente. Dovrà poi essere impostato un risponditore automatico (non quindi un inoltro a terzi ma una risposta al solo mittente) comunicando che l'account è disattivato e che potrà contattare l'indirizzo di altro dipendente, alternativo rispetto a quello inizialmente selezionato (ad esempio: "tizio@lamiascuola.it è un account disattivato, prego scrivere a caio@lamiascuola.it").
Tale risponditore dovrà restare in funzione per un tempo determinato e assolutamente non eccedente rispetto alle esigenze di continuità. Al termine di questo periodo transitorio dovrà seguire la rimozione dell'account.

COME UTILIZZARE CORRETTAMENTE LE E-MAIL

In caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica (anche nell'ambito del Sistema di Gestione EUservice) e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

In ogni caso, si devono rispettare le seguenti istruzioni:

UTILIZZARE ESCLUSIVAMENTE LE MAIL ISTITUZIONALI PER LE COMUNICAZIONI

PRIMA DELL'INVIO:

1. Controllare almeno due volte (double-check) oltre al corpo mail anche allegato, destinatario etc.
2. CCN in caso di comunicazione a molteplici destinatari

ALLA RICEZIONE DI UN MESSAGGIO:

1. Controllare sempre l'indirizzo del mittente e verificarne sempre l'attendibilità. In caso di mittente non attendibile non aprire mai allegati alla mail, né cliccare su link presenti.

Copyright 2022
EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale

Nel caso in cui anche una sola delle sopra indicate istruzioni non fosse stata eseguita correttamente si consiglia di contattare tempestivamente il DPO.

TRATTAMENTO DEI METADATI

TRATTAMENTO DEI METADATI E LIMITI AI CONTROLLI SULL'ATTIVITÀ DEI LAVORATORI

Nell'ambito dell'utilizzo degli strumenti informatici messi a disposizione per lo svolgimento dell'attività lavorativa (quali, a titolo esemplificativo, sistemi di posta elettronica, piattaforme digitali e infrastrutture informatiche), il Datore di lavoro può trattare esclusivamente i metadati e i log tecnici strettamente necessari ad assicurare il corretto funzionamento dei sistemi, la sicurezza informatica e la tutela del patrimonio informativo dell'Istituto. Tale trattamento avviene nel rispetto dell'art. 4, comma 2, della Legge n. 300/1970 (Statuto dei Lavoratori) ed è limitato agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa o per la registrazione di accessi e presenze. In tale ambito, la raccolta e la conservazione dei metadati non è finalizzata al controllo dell'attività lavorativa, né alla valutazione individuale delle prestazioni. I metadati (quali, a titolo esemplificativo, informazioni relative a data e ora di invio o ricezione, mittente e destinatario, log di accesso ai sistemi) sono trattati secondo i principi di liceità, correttezza, trasparenza, minimizzazione e limitazione della conservazione, e sono conservati, di norma, per un periodo limitato e proporzionato, normalmente non superiore a 21 giorni, salvo la comprovata necessità di una conservazione più estesa per specifiche esigenze tecniche o di sicurezza, adeguatamente documentate nel rispetto del principio di responsabilizzazione (accountability). È esclusa qualsiasi forma di raccolta generalizzata o conservazione prolungata dei metadati che possa comportare, anche indirettamente, un controllo a distanza dell'attività dei lavoratori, salvo il rispetto delle garanzie procedurali previste dall'art. 4, comma 1, dello Statuto dei Lavoratori (accordo sindacale o autorizzazione dell'autorità competente).
Il Datore di lavoro si impegna a:
limitare l'accesso ai metadati ai soli soggetti espressamente autorizzati e adeguatamente istruiti;

- garantire la tracciabilità degli accessi ai dati;
- adottare misure tecniche e organizzative idonee a prevenire utilizzi impropri o eccedenti le finalità dichiarate;
- assicurare che eventuali fornitori di servizi informatici, inclusi quelli in modalità cloud, trattino i dati personali esclusivamente sulla base delle istruzioni ricevute e nel rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita.

I lavoratori sono informati che dai metadati non possono essere desunte né utilizzate informazioni attinenti alla sfera personale, alle opinioni politiche, religiose o sindacali, né fatti non rilevanti ai fini dell'attività lavorativa, restando in ogni caso vietate indagini eccedenti i limiti consentiti dalla normativa vigente.
Ogni trattamento dei metadati avviene nel rispetto della normativa in materia di protezione dei dati personali e della disciplina sui controlli a distanza, e può essere utilizzato dal Datore di lavoro per finalità connesse alla gestione del rapporto di lavoro solo se i dati sono stati lecitamente raccolti e nel rispetto delle presenti disposizioni.

Copyright 2022
EUSERVICE s.r.l. - via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008
Quest'opera è distribuita con Licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale