ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

# Disciplinare interno sull'utilizzo degli strumenti informatici

ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

## Sommario

## 1. Adozione del Disciplinare e pubblicità

1.1 In seguito all'adozione del presente Disciplinare, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

1.2 Del presente disciplinare viene fornita massima pubblicità e diffusione mediante la sua pubblicazione nel sito internet dell'Istituto e tramite invio in allegato attraverso la mailing list del personale INDIRE.

## 2. Campo di applicazione del Disciplinare

2.1 Il nuovo Disciplinare si applica a tutto il personale dipendente, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti dell'Istituto, indipendentemente dalla natura del rapporto contrattuale, autorizzati a far uso di strumenti tecnologici dell'Istituto o ad accedere alla rete informatica e ad eventuali dati ed informazioni ivi conservati e trattati.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "**utente**" deve intendersi ogni dipendente, collaboratore e/o consulente in possesso di specifiche credenziali di autenticazione. Ogni utente potrà essere designato quale "autorizzato al trattamento" o "referente privacy" ovvero "amministratore di sistema", ai sensi di quanto previsto dal GDPR, dal Codice Privacy e dagli specifici provvedimenti in materia del Garante Privacy, in ragione delle specifiche attività e funzioni che ciascun utente ricopre all'interno dell'Istituto come da organigramma e da contratto.

## 3. Utilizzo del Personal Computer

3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo contrario alle finalità dell'attività lavorativa è vietato al fine di evitare eventuali disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e possibile *data breach*. Il personal computer deve essere custodito con cura da parte degli utenti assegnatari evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Istituto solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Disciplinare.

3.3 L'Istituto rende noto che il personale (anche esterno) addetto ai servizi informatici e gli Amministratori di Sistema (di seguito congiuntamente definiti "**Servizio IT**") designati sono stati autorizzati a compiere interventi nel sistema informatico dell'Istituto diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).
La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il Servizio IT ne darà idonea comunicazione agli utenti interessati.

3.4 Il personale incaricato del Servizio IT ha la facoltà di collegarsi e visualizzare in remoto i contenuti 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 comunicazione della necessità dell'intervento stesso.

3.5 Salvo autorizzazione del Servizio IT, non è consentito l'utilizzo di programmi – o servizi applicativi via internet – diversi da quelli ufficialmente approvati dall'Istituto o installati dal personale del Servizio IT né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti o di violare diritti di proprietà intellettuale.

L'inosservanza della presente disposizione espone l'Istituto a potenziali 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 programmi per elaboratore regolarmente licenziati, o comunque liberi e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Istituto.

3.6 Salvo preventiva autorizzazione del personale del Servizio IT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi esterni di memorizzazione personali, comunicazione o altro.

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Disciplinare relativo alle procedure di protezione antivirus.

3.8 Salvo i casi espressamente autorizzati, il Personal Computer deve essere bloccato ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

## 4. Assegnazione e gestione e delle credenziali di autenticazione e autorizzazione

4.1 Le credenziali di autenticazione, ivi incluse quelle per i sistemi gestionali in uso presso INDIRE, vengono assegnate dagli amministratori di sistema e dal personale del Servizio IT, previa espressa indicazione della Direzione ovvero previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
È proibito utilizzare le funzioni applicative ad accesso controllato con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente ("*USER ID"*), assegnato dal Servizio IT, associato ad una parola chiave ("*PASSWORD*") riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri e/o caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri alfanumerici e non deve contenere riferimenti agevolmente riconducibili all'utente.

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di "dati sensibili" attraverso l'ausilio di strumenti elettronici).

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio IT.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è l'Amministratore di Sistema e il personale incaricato del Servizio IT.

## 5. Utilizzo della rete informatica e gestione dei dati nelle postazioni di lavoro

5.1 Le cartelle di rete, personali o condivise, possono ospitare informazioni esclusivamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e backup da parte del personale del Servizio IT.
Eventuale materiale personale non autorizzato rilevato dal Servizio IT nel corso dei predetti interventi di sicurezza informatica ovvero di manutenzione/aggiornamento verrà rimosso in osservanza di quanto disposto dal presente disciplinare.

5.2 Il personale del Servizio IT, ove necessario, potrà in qualunque momento procedere alla rimozione di ogni file o applicazione pericolosi per la Sicurezza dell'Istituto sia sui PC degli utenti sia sulle unità di rete.

5.3 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario, in osservanza del principio di minimizzazione dei dati ex art. 5, lett. C del GDPR, evitare archiviazioni ridondanti o non pertinenti rispetto alle finalità per cui i dati sono trattati.

5.4 Nella gestione dei sistemi informatici dell'Istituto, il Servizio IT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, nei limiti di quanto previsto nel presente Disciplinare, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

5.5 Senza la debita autorizzazione, è vietato trasferire documenti elettronici contenenti dati personali o informazioni riservate dai sistemi informatici dell'Istituto a device esterni (quali ad

es. hard disk, chiavette, CD, DVD e altri supporti) nonché salvare documenti elettronici dell'Istituto (ad esempio pervenuti via mail o salvati sul Server o su SPC Cloud) su repository esterne (quali ad es. Dropbox, GoogleDrive, OneDrive, Youtube, ecc.) ovvero inviarli a terzi via posta elettronica o con altri sistemi per finalità estranee all'attività lavorativa.

## 6. Utilizzo di altri dispositivi elettronici

6.1 Tutti i dispositivi elettronici dati in dotazione al personale dell'Istituto devono considerarsi strumenti di lavoro: ne viene concesso l'uso per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere prevalentemente personale o comunque non strettamente inerenti le attività lavorative.

6.2 Particolare attenzione deve essere prestata quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o persino sensibili o giudiziari in quanto occorre evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa. L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare.
Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

## 7. Utilizzo e conservazione dei supporti rimovibili

7.1 Tutti i supporti rimovibili (CD e DVD riscrivibili, supporti USB, hard disk esterni, ecc.), contenenti dati personali o sensibili nonché informazioni riservate dell'Istituto, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati dell'Istituto in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi o scaffali chiusi a chiave, ove disponibili.

7.3 È vietato l'utilizzo di supporti rimovibili personali.

7.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio IT e seguire le istruzioni da questo impartite.
Nel caso di dispositivi elettronici, con riferimento in particolare a eventuali PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del Servizio IT.

## 8. Uso della posta elettronica

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È vietato utilizzare le caselle di posta elettronica dell'Istituto 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:

*(i)* l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;

*(ii)* l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

*(iii)* la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al

personale del Servizio IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza lavorativa e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica e i documenti non pertinenti all'attività lavorativa e non utili alle esigenze dell'Istituto, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente all'attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dall'Istituto quale corrispondenza e documentazione lavorativa e non personale.

8.4 È obbligatorio porre la massima attenzione nell'aprire i file *attachments* (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti), evitando possibilmente di aprire messaggi di posta in arrivo da mittenti di cui non sin conosce l'identità o con contenuto sospetto o insolito.
È altresì obbligatorio prestare grande attenzione alla credibilità del messaggio e del mittente per evitare casi di *phishing* o frodi informatiche. In casi di incertezza si raccomanda di contattare il Servizio IT.

8.5 Nel caso in cui si renda necessario inviare a destinatari esterni messaggi contenenti allegati con dati "sensibili" o "giudiziari" (ex artt. 9 e 10 GDPR), è obbligatorio che questi documenti vengano preventivamente resi inintelligibili attraverso tecniche di cifratura con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati.

8.6 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione *autoreply* o l'inoltro automatico su altre caselle dell'Istituto e si debba conoscere il contenuto dei messaggi di posta elettronica, l'utente assegnatario della casella di posta deve delegare un altro collega (fiduciario) per

verificare il contenuto di messaggi e per inoltrare al responsabile di settore o alla Direzione Generale quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del responsabile di settore assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato l'utente interessato alla prima occasione utile.

8.7 La corrispondenza in entrata viene sistematicamente analizzata dai software antivirus e antispam in dotazione presso l'Istituto. I messaggi infetti saranno eliminati automaticamente dal sistema.

8.8 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 che ne giustificava l'assegnazione.

L'Istituto si riserva, tuttavia, di valutare a proprio esclusivo e insindacabile giudizio la necessità di mantenere attiva solamente in ricezione la casella per un periodo di tempo massimo di sei mesi dalla cessazione del rapporto lavorativo al fine di garantire la funzionalità lavorativa; in tal caso:

*(i)* avrà accesso alla casella esclusivamente un altro utente appositamente designato dall'Istituto in funzione alle mansioni lavorative assegnate;

*(ii)* Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail dell'Istituto.

8.9 Nel caso in cui venisse assegnata all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di titolarità dell'Istituto, tale utente dovrà attenersi alle regole previste nelle ulteriori specifiche istruzioni a ciò dedicate e che andranno a completare e integrare le disposizioni del presente Disciplinare.

## 9. Navigazione in Internet

9.1 Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento professionale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

9.2 A tale riguardo, è vietato compiere azioni che possano arrecare un danno all'Istituto, ovvero limitare le legittime attività di protezione poste in essere dall'Istituto, ad esempio:

*(i)* il download e l'upload di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web (filmati e musica) per finalità personali o comunque estranee all'attività lavorativa (salvo il caso di previa autorizzazione del Servizio IT);

*(ii)* l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del Servizio IT) e comunque nel rispetto delle normali procedure di acquisto;

*(iii)* ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

*(iv)* la partecipazione a forum non professionali, l'iscrizione con account INDIRE e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dalla Direzione;

*(v)* l'apertura di canali ufficiali dell'Istituto c/o social network o piattaforme web se non espressamente autorizzati dalla Direzione.

9.3 L'Istituto si riserva di bloccare l'accesso a siti non attinenti l'attività lavorativa o considerati "a rischio" attraverso l'utilizzo di *blacklist* pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell'Istituto, si prega di contattare il Servizio IT per uno sblocco selettivo.

9.4 I sistemi software di monitoraggio e controllo sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet

e al traffico telematico la cui conservazione non sia necessaria. Gli eventuali controlli, compiuti dal personale incaricato del Servizio IT per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (*Proxy server*) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo e i file stessi in ogni caso vengono conservati non oltre sei mesi.

Un eventuale ed eccezionale prolungamento dei tempi di conservazione può aver luogo solo in relazione ad esigenze tecniche o di sicurezza del tutto particolari (ad. es. per indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; per obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria, ecc.).

9.5 Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

9.6 L'utilizzo di tutte le reti WiFi presenti presso l'Istituto è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile sarà possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal Servizio IT.

9.7 L'accesso da remoto alla rete dell'Istituto è possibile agli utenti solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che li abilitino sui dispositivi in uso.

## 10. Protezione antivirus

10.1 Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'Istituto mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio IT.

## 11. Comunicazione e/o pubblicazione di prodotti audiovisivi e delle buone pratiche didattiche ed educative

11.1 L'utente, prima di realizzare, documentare, conservare e/o divulgare materiali audio-visivi contenenti i dati personali degli interessati (studenti, professori, famiglie, ecc.) deve accertarsi, in via preliminare, che tali attività di trattamento siano effettivamente necessarie al perseguimento di specifiche finalità istituzionali dell'INDIRE o all'esecuzione di obbligazioni contrattuali assunte oppure espressamente previste dalla normativa di settore.

11.2 Tutti gli "interessati" (studenti, famiglie, professori, ecc.) hanno il diritto di conoscere come il Titolare (che può essere l'Istituto, o il MIUR, o le singole scuole o finanche persone fisiche quali i docenti) tratti i loro dati personali. Il Titolare (direttamente o per mezzo del Responsabile esterno del trattamento laddove nominato) deve dunque in ogni caso rendere noto, attraverso un'adeguata **informativa**, quali dati sono raccolti, come sono utilizzati e a quale fine. A tale riguardo l'utente, prima di realizzare, documentare, conservare e/o divulgare materiali audio-visivi contenenti i dati personali, deve accertarsi, ove possibile, che sia stata fornita l'informativa all'interessato e salvarla in una directory dedicata indicata dall'Istituto ovvero in archivio cartaceo.

Laddove le informative siano state rilasciate agli interessati da altri enti o soggetti Titolari, e non siano in possesso dell'Istituto, l'utente deve raccogliere e conservare in una directory dedicata le dichiarazioni del Titolare (ad es. dirigente scolastico e/o docente) attestanti che tutti gli interessati hanno ricevuto idonea informativa, con facoltà di INDIRE di acquisire a richiesta la documentazione in originale.

11.3 Particolare attenzione deve essere prestata dall'utente all'eventuale pubblicazione di immagini e/o video su Internet, e sui social network in particolare. In caso di **comunicazione** o

**diffusione** diventa infatti necessario, di regola, ottenere il **consenso** informato delle persone rappresentate nelle fotografie e nei video.

Ai sensi dell'art. 2-ter del Codice Privacy:

(i) per "**comunicazione**" si intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione";

(ii) per "**diffusione**" si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

In tali casi l'utente deve accertarsi che ciascun interessato abbia espressamente manifestato il proprio consenso alle specifiche attività di comunicazione e/o diffusione delle proprie immagini, anche mediante pubblicazione delle stesse sui social network, sottoscrivendo apposita **dichiarazione liberatoria** predisposta dal Titolare del trattamento e fornita dal Titolare stesso o per mezzo del Responsabile esterno del trattamento, laddove nominato, ai sensi della vigente normativa in materia di protezione dei dati personali e sul diritto d'autore.

Le dichiarazioni liberatorie all'utilizzo e diffusione delle immagini devono essere salvate dall'utente e conservate in una directory dedicata indicata dall'Istituto ovvero in archivio cartaceo.

Laddove le liberatorie firmate siano state rilasciate agli interessati da altri enti o soggetti Titolari, e non siano in possesso dell'Istituto, l'utente deve raccogliere e conservare in una directory dedicata le dichiarazioni del Titolare (ad es. dirigente scolastico e/o docente) attestanti che tutti gli interessati hanno sottoscritto idonea liberatoria con facoltà di INDIRE di acquisire a richiesta la documentazione in originale.

11.4 In caso di minori, al fine di garantire la liceità del trattamento, l'utente deve assicurarsi che il consenso alla comunicazione e/o diffusione di immagini/video sia stato prestato da chi ne esercita la responsabilità genitoriale mediante sottoscrizione di apposito modulo fornito dall'Istituto o in generale dal Titolare del trattamento. Occorre precisare che, ai sensi dell'articolo 2-quinquies del Codice Privacy, è valido il consenso del minore che ha compiuto quattordici anni limitatamente all'offerta di "**servizi della società dell'informazione[1]".**

[1] L'articolo 4, numero 25, del GDPR definisce: «**servizio della società dell'informazione**» il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, e dunque:

11.5 Nel caso in cui un interessato (studente, familiare, docente, ecc.) non abbia prestato il proprio specifico consenso alla diffusione dei propri dati personali, l'utente, prima di pubblicare materiale audio-visivo raffigurante detto interessato, ove occorra con l'aiuto del settore IT, dovrà utilizzare un software indicato dall'Istituto che consenta di oscurare ("*pixelare*") il volto del soggetto in questione, rendendolo di fatto non identificabile nel rispetto della normativa in materia di protezione dei dati personali.

11.6 In osservanza del principio di minimizzazione dei dati e del principio di "Privacy by default" di cui all'art. 25, comma 2, del GDPR, si raccomanda all'utente di fare ricorso a piattaforme esterne o a social network laddove vi sia una necessità di divulgazione virale dei prodotti audiovisivi e/o delle buone pratiche educative che non possa essere pienamente soddisfatta mediante pubblicazione degli stessi all'interno dei siti web istituzionali di INDIRE.

11.7 Alcune categorie particolari di dati personali degli interessati – altrimenti noti come "dati sensibili" (si pensi ad. es. alle convinzioni religiose, all'origine razziale o etnica, ecc.) – devono essere trattate con estrema cautela, nel rispetto del GDPR e del Codice Privacy, verificando prima non solo la pertinenza dei dati ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire mediante la pubblicazione di materiale audiovisivo e/o delle buone pratiche educative.

La pubblicazione di dati relativi allo stato di salute degli interessati (si pensi ad. es. ad alunni disabili o con disturbi specifici di apprendimento – DSA – o con bisogni educativi speciali – BES) è di regola sempre vietata, fatte salve eccezionali ipotesi concordate preventivamente

---

b) «**servizio**»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

Ai fini della presente definizione si intende per:

i) «**a distanza**»: un servizio fornito senza la presenza simultanea delle parti;
ii) «**per via elettronica**»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;
iii) «**a richiesta individuale di un destinatario di servizi**»: un servizio fornito mediante trasmissione di dati su richiesta individuale;

con la Direzione, sentito il parere del DPO, e previa informata, esplicita e specifica manifestazione di consenso da parte del diretto interessato o di chi ne esercita la responsabilità genitoriale.

11.8 Restano ferme ed impregiudicate le specifiche prerogative e funzioni degli archivisti dell'Istituto, i quali in ogni caso, dovranno attenersi altresì, oltre che alle disposizioni del GDPR e del Codice Privacy (cfr. in particolare artt. 101-103), alle Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate nella Gazzetta Ufficiale n. 12 del 15.01.19 e ss. mm. ii.
Si rammenta che i dati personali trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, ai sensi dell'art. 101 III comma del Codice Privacy, possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico.

## 12. Osservanza delle disposizioni in materia di protezione dei dati personali e Statuto dei Lavoratori

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e alle istruzioni operative per il trattamento dei dati, come indicato nella lettera di designazione a "persona autorizzata al trattamento dei dati" ex art. 4, paragrafo 10, GDPR nonché ex art. 2 *quaterdecies* del Codice Privacy.

12.2 Gli strumenti tecnologici considerati nel presente Disciplinare 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 ("Statuto dei Lavoratori"). Le informazioni raccolte sulla base di quanto indicato nel Disciplinare, anche conformemente al successivo punto 13, potranno essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendo stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico dell'Istituto ovvero nel singolo strumento e sui

conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto del GDPR e del Codice Privacy.

12.3 Si precisa che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori.

## 13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi sostenuti dall'Istituto (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Generale, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della vigente normativa in materia di protezione dei dati personali e delle procedure di cui ai precedenti 3.3 e 3.4, a tutti gli strumenti informatici dell'Istituto e ai documenti ivi contenuti.

## 14. Graduazione dei controlli

14.1 In caso di anomalie, nel rispetto dei principi di pertinenza e non eccedenza, il personale incaricato del Servizio IT potrà effettuare controlli anonimi sull'uso degli strumenti elettronici che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## 15. Sanzioni

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate da parte del personale dipendente è sanzionabile con eventuali provvedimenti previsti dal vigente CCNL del comparto di riferimento e dalla normativa vigente.

## 16. Aggiornamento e revisione

16.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Disciplinare. Le proposte verranno esaminate dalla Direzione Generale.

16.2 Il presente Disciplinare è soggetto periodicamente a revisione.