



Linee guida interne sull'utilizzo di sistemi documentali a norma su server DNSH-compliant

Approvate dal Consiglio d'Istituto con delibera n. 122 del 23 febbraio 2026

Sistemi realizzati grazie al finanziamento PNRR Codice avviso/decreto M4C1I3.2-2022-961 - Piano Scuola 4.0 - Azione 1 - Next generation class - Ambienti di apprendimento innovativi - progetto M4C1I3.2-2022-961-P-17356, codice CUP H74D22004250006 - Titolo progetto Next generation classes @IC E.Fermi - Carvico

1. Introduzione

La trasformazione digitale delle istituzioni scolastiche rappresenta un fattore strategico per il miglioramento dell'organizzazione amministrativa, della didattica e dei processi di collaborazione interna, nel rispetto dei principi di legalità, trasparenza e sostenibilità.

Nell'ambito degli interventi finanziati dal **Piano Nazionale di Ripresa e Resilienza (PNRR)**, l'Istituzione scolastica ha adottato un **sistema documentale complementare** a supporto della condivisione e della gestione di documenti informatici per finalità amministrative e didattiche, integrato con i sistemi istituzionali già in uso e ospitato su **infrastruttura server DNSH-compliant**.

L'utilizzo di strumenti digitali per la gestione documentale comporta il trattamento di dati personali e l'impiego di infrastrutture tecnologiche che hanno un impatto, seppur indiretto, sull'ambiente. Per tale motivo, è necessario definire un quadro chiaro di **regole, responsabilità e buone pratiche** che garantisca:

- il rispetto della **normativa europea e nazionale in materia di protezione dei dati personali**;
- la corretta distinzione tra gestione documentale operativa e **conservazione digitale a norma**;
- la sicurezza delle informazioni e la tutela dei diritti degli interessati;
- la conformità al principio **DNSH – Do No Significant Harm**, quale requisito essenziale per i progetti finanziati con risorse PNRR.

Le presenti **Linee guida interne** sono state redatte con l'obiettivo di fornire un riferimento unitario e condiviso per tutti i soggetti autorizzati all'utilizzo del sistema documentale complementare, definendo criteri organizzativi, tecnici e comportamentali coerenti con il ruolo pubblico dell'Istituzione scolastica.

Il documento non disciplina l'uso di sistemi di Intelligenza Artificiale, in quanto il sistema documentale adottato **non utilizza né integra funzionalità di IA**, né prevede processi decisionali automatizzati.

Le Linee guida costituiscono pertanto uno strumento di **governance interna**, a supporto dell'azione amministrativa e didattica della scuola, e rappresentano parte integrante delle misure di responsabilizzazione, controllo e rendicontazione richieste dalla *compliance* normativa di settore.

Le piattaforme del sistema di gestione documentale complementare sono state realizzate grazie ai finanziamenti PNRR Codice avviso/decreto M4C1I3.2-2022-961 - Piano Scuola 4.0 - Azione 1 - Next generation class - Ambienti di apprendimento innovativi - progetto M4C1I3.2-2022-961-P-17356, codice CUP H74D22004250006 - Titolo progetto Next generation classes @IC E.Fermi - Carvico.

1.1 Finalità del documento

Le presenti Linee guida interne hanno lo scopo di definire i criteri organizzativi, tecnici e procedurali per il corretto utilizzo del sistema documentale complementare al sistema Gecodoc e al Registro Elettronico per la condivisione di documenti informatici sia per finalità amministrative che didattiche, adottato dall'Istituzione scolastica, realizzato con fondi del Piano Nazionale di Ripresa e Resilienza (PNRR) e ospitato su infrastruttura server DNSH-compliant.

Il documento è finalizzato a:

- garantire la conformità del sistema documentale alla normativa europea e nazionale in materia di protezione dei dati personali, con particolare riferimento ai principi di liceità, correttezza, trasparenza, sicurezza e responsabilizzazione;
- assicurare una gestione documentale a norma, nel rispetto delle disposizioni vigenti in materia di formazione e gestione dei documenti digitali dell'Istituto comprensivo. Sono esclusi dall'utilizzo del sistema documentale complementare tutti i documenti oggetto di archiviazione e conservazione a norma;
- esplicitare le modalità operative idonee a prevenire trattamenti non autorizzati o impropri di dati personali, inclusi i dati relativi a studenti, famiglie, personale docente e ATA;
- attestare il rispetto del principio DNSH – "Do No Significant Harm", dimostrando che l'adozione e l'utilizzo del sistema documentale non arrecano danni significativi all'ambiente, in coerenza con gli obiettivi ambientali previsti dal quadro normativo europeo e dagli interventi PNRR;
- fornire un riferimento interno univoco per dirigenti, personale amministrativo, tecnico e utenti autorizzati, al fine di assicurare uniformità di comportamento, tracciabilità delle operazioni e riduzione dei rischi operativi e normativi.

Le Linee guida costituiscono pertanto uno strumento di governance interna, a supporto dell'azione amministrativa della scuola, e rappresentano parte integrante del sistema di controllo e di responsabilizzazione richiesto per la gestione dei documenti informatici.

1.2 Ambito di applicazione

Le presenti Linee guida si applicano all'utilizzo del **sistema documentale complementare** adottato dall'Istituzione scolastica per la **condivisione e gestione di documenti informatici**, sia per **finalità amministrative** sia per **finalità didattiche**, in integrazione con il sistema **Gecodoc** e con il **Registro Elettronico**.

Rientrano nell'ambito di applicazione delle Linee guida:

- i documenti informatici prodotti o condivisi dall'Istituto comprensivo per esigenze organizzative, gestionali, didattiche e collaborative o dai Comitati Genitori in attività preventivamente condivise con l'Istituto comprensivo.

I documenti possono contenere dati personali di studenti, famiglie, personale docente e personale ATA, trattati nell'ambito delle attività istituzionali della scuola, previa specifica

acquisizione, quando richiesto, del consenso al trattamento dati da parte degli interessati;

- gli utenti autorizzati all'accesso e all'utilizzo del sistema documentale complementare, inclusi il Dirigente scolastico, il personale amministrativo, il personale docente, il personale tecnico e ogni altro soggetto formalmente autorizzato.

Sono **espressamente esclusi** dall'ambito di applicazione delle presenti Linee guida:

- i documenti soggetti a **protocollo informatico**, archiviazione e **conservazione digitale a norma**, che continuano a essere gestiti esclusivamente tramite i sistemi istituzionali preposti (Gecodoc e altri sistemi conformi alla normativa vigente);
- i trattamenti di dati personali effettuati mediante strumenti o piattaforme diverse dal sistema documentale complementare oggetto del presente documento.

Le Linee guida si applicano esclusivamente alle **modalità di utilizzo, gestione e sicurezza** del sistema documentale complementare e non sostituiscono né modificano le disposizioni normative, regolamentari o contrattuali vigenti in materia di gestione documentale, protezione dei dati personali e utilizzo degli strumenti digitali dell'Istituzione scolastica.

1.3 Destinatari delle Linee guida

Le presenti Linee guida sono rivolte a tutti i soggetti che, a vario titolo, sono **autorizzati ad accedere e utilizzare il sistema documentale complementare** adottato dall'Istituzione scolastica, nell'ambito delle attività istituzionali, amministrative e didattiche.

In particolare, sono destinatari delle Linee guida:

- **il Dirigente scolastico**, in qualità di responsabile dell'organizzazione complessiva del sistema documentale e garante del rispetto delle disposizioni normative e interne;
- **il personale amministrativo**, per le attività di gestione, condivisione e consultazione della documentazione amministrativa e organizzativa;
- **il personale docente**, per le attività didattiche, collaborative e di supporto alla funzione educativa, nei limiti delle autorizzazioni assegnate;
- **il personale tecnico e ATA**, per le attività connesse al supporto operativo e tecnico del sistema, secondo i profili di accesso attribuiti;
- **altri utenti interni** espressamente individuati e autorizzati, in relazione a specifiche esigenze organizzative o progettuali;
- **i Responsabili dei Comitati Genitori**, esclusivamente previa **formale autorizzazione del Dirigente scolastico**, limitatamente alle attività di consultazione e condivisione di documenti strettamente connessi alle iniziative e ai progetti di competenza dei Comitati stessi.

L'accesso al sistema documentale complementare da parte di ciascun destinatario è subordinato a:

- attribuzione di **specifici profili di autorizzazione**, coerenti con il ruolo e le funzioni svolte;
- rispetto delle presenti Linee guida e delle ulteriori disposizioni interne in materia di sicurezza informatica e protezione dei dati personali;
- osservanza degli obblighi di **riservatezza e corretto utilizzo** delle informazioni e dei documenti trattati.

Ogni utilizzo del sistema documentale al di fuori delle finalità istituzionali e delle autorizzazioni assegnate è da considerarsi **non conforme** e potenzialmente rilevante ai fini disciplinari e normativi.

1.4 Definizioni e acronimi

Ai fini delle presenti Linee guida, si applicano le seguenti definizioni e acronimi.

Sistema documentale complementare

Piattaforma digitale adottata dall'Istituzione scolastica per la condivisione e gestione di documenti informatici a supporto delle attività amministrative e didattiche, distinta e complementare rispetto ai sistemi di protocollo, archiviazione e conservazione a norma.

Documento informatico

Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, formata, gestita e conservata secondo le disposizioni normative vigenti.

Gecodoc

Sistema di gestione documentale utilizzato dall'Istituzione scolastica per il protocollo informatico e la gestione dei documenti soggetti ad archiviazione e conservazione a norma.

Registro Elettronico

Sistema informatico utilizzato per la gestione delle attività didattiche e amministrative connesse alla vita scolastica, compresa la comunicazione con studenti e famiglie.

Dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, mediante riferimento a uno o più elementi identificativi.

Trattamento dei dati personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di strumenti informatici, applicate a dati personali, quali la raccolta, la registrazione, la conservazione, la consultazione, la comunicazione o la cancellazione.

Titolare del trattamento

Il soggetto che determina le finalità e i mezzi del trattamento dei dati personali. Nel contesto delle presenti Linee guida, il Titolare del trattamento è l'Istituzione scolastica, nella persona del Dirigente scolastico.

Utente autorizzato

Soggetto che, sulla base di un ruolo formalmente attribuito, è abilitato ad accedere al sistema documentale complementare e a trattare documenti e dati personali nei limiti delle autorizzazioni assegnate.

DNSH (Do No Significant Harm)

Principio secondo cui un'attività economica o un intervento finanziato non deve arrecare danni significativi agli obiettivi ambientali definiti dalla normativa europea.

Server DNSH-compliant

Infrastruttura tecnologica conforme ai requisiti di sostenibilità ambientale e di efficienza energetica richiesti dal principio DNSH, utilizzata per l'ospitare il sistema documentale complementare.

PNRR (Piano Nazionale di Ripresa e Resilienza)

Strumento di programmazione e finanziamento nazionale volto all'attuazione degli interventi previsti dal programma europeo Next Generation EU.

Linee guida

Il presente documento interno che disciplina l'utilizzo del sistema documentale complementare e ne definisce i criteri di conformità normativa, organizzativa e ambientale.

2.1 Normativa europea sulla protezione dei dati personali

La principale fonte europea in materia di protezione dei dati personali è il **Regolamento (UE) 2016/679**, comunemente noto come **Regolamento generale sulla protezione dei dati (GDPR)**. Si tratta di un **atto normativo direttamente applicabile in tutti gli Stati membri dell'Unione Europea**, entrato in vigore il **25 maggio 2018**, con l'obiettivo di tutelare la protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

Il GDPR disciplina i principi, i diritti e gli obblighi relativi al trattamento dei dati personali da parte di enti pubblici e privati e stabilisce un quadro uniforme di regole nel territorio dell'Unione europea, con efficacia diretta senza necessità di recepimento da parte degli Stati membri.

In particolare, il GDPR si fonda su alcuni **principi chiave** che l'Istituzione scolastica deve rispettare nell'ambito dei trattamenti di dati personali effettuati tramite il sistema documentale complementare:

- **Liceità, correttezza e trasparenza** del trattamento dei dati;
- **Limitazione delle finalità**, con dati raccolti per scopi determinati e legittimi;
- **Minimizzazione dei dati**, prevedendo l'utilizzo di soli dati pertinenti e necessari;
- **Esattezza** dei dati conservati e aggiornamento tempestivo;
- **Limitazione della conservazione**, con definizione di tempi di retention adeguati;

- **Integrità e riservatezza**, garantendo un'adeguata sicurezza tecnica e organizzativa.

Il GDPR riconosce inoltre **diritti specifici agli interessati**, quali il diritto di accesso, rettifica, cancellazione o limitazione del trattamento, nonché il diritto alla portabilità dei dati, che devono essere assicurati dall'Istituzione scolastica nei limiti e nelle modalità previsti dallo stesso Regolamento.

2.2 Normativa nazionale di recepimento e disposizioni applicabili

Il quadro normativo europeo in materia di protezione dei dati personali trova applicazione nell'ordinamento italiano attraverso una serie di disposizioni nazionali che **integrano e specificano** il Regolamento (UE) 2016/679, con particolare riferimento al contesto delle pubbliche amministrazioni e delle istituzioni scolastiche.

In particolare, costituisce riferimento fondamentale:

- il **Decreto legislativo 30 giugno 2003, n. 196**, recante il *Codice in materia di protezione dei dati personali*, come **modificato e integrato dal Decreto legislativo 10 agosto 2018, n. 101**, che ha adeguato l'ordinamento nazionale alle disposizioni del GDPR.

Il Codice così novellato disciplina:

- le condizioni di liceità del trattamento dei dati personali da parte dei soggetti pubblici;
- le modalità di esercizio dei diritti degli interessati;
- le misure di garanzia per il trattamento di categorie particolari di dati;
- il ruolo e i poteri dell'Autorità Garante per la protezione dei dati personali.

Per quanto riguarda il settore scolastico, assumono particolare rilevanza:

- le disposizioni che regolano il trattamento dei dati personali per l'esecuzione di **compiti di interesse pubblico o connessi all'esercizio di pubblici poteri**, cui rientrano le funzioni istituzionali dell'Istituzione scolastica;
- le norme in materia di **dati relativi a minori**, che richiedono un livello di attenzione e tutela rafforzato;
- gli obblighi di sicurezza e di responsabilizzazione del titolare del trattamento, con particolare riferimento all'adozione di misure tecniche e organizzative adeguate.

Sono inoltre applicabili:

- le disposizioni in materia di **amministrazione digitale**, contenute nel **Codice dell'Amministrazione Digitale (CAD)**, per quanto attiene alla formazione, gestione e trasmissione dei documenti informatici;

- le linee guida e i provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali, in quanto atti di indirizzo e interpretazione per le pubbliche amministrazioni;
- le disposizioni specifiche in materia di **trasparenza, accesso agli atti e protezione dei dati personali**, nella misura in cui risultino compatibili con le finalità del sistema documentale complementare.

L'applicazione delle presenti Linee guida avviene pertanto nel rispetto del **quadro normativo nazionale vigente**, che integra la disciplina europea e ne garantisce l'attuazione concreta all'interno dell'Istituzione scolastica.

2.3 Normativa sulla gestione documentale e conservazione digitale

La gestione dei documenti informatici all'interno dell'Istituzione scolastica è disciplinata da un complesso di norme nazionali che regolano la **formazione, gestione, trasmissione, archiviazione e conservazione** dei documenti della Pubblica Amministrazione.

Il riferimento principale è costituito dal **Codice dell'Amministrazione Digitale (CAD)**, di cui al Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni, che stabilisce i principi generali per la gestione dei documenti informatici, l'utilizzo delle tecnologie digitali e la validità giuridica degli atti della Pubblica Amministrazione.

In attuazione del CAD, assumono particolare rilievo:

- le **Linee guida sulla formazione, gestione e conservazione dei documenti informatici**, adottate dall'Agenzia per l'Italia Digitale (AgID), che definiscono:
 - i requisiti per la formazione dei documenti informatici;
 - le modalità di gestione dei flussi documentali;
 - i criteri per l'archiviazione e la conservazione digitale a norma;
- le disposizioni relative al **protocollo informatico**, alla classificazione e alla fascicolazione dei documenti.

Nel contesto delle presenti Linee guida, il **sistema documentale complementare**:

- è utilizzato esclusivamente per la **gestione operativa e la condivisione di documenti informatici** a supporto delle attività amministrative e didattiche ovvero per la promozione interna delle attività dei Comitati Genitori;
- **non sostituisce** né integra i sistemi di **protocollo informatico**, archiviazione e **conservazione digitale a norma**, che restano disciplinati dalle specifiche normative e affidati agli strumenti istituzionali preposti;

- non è destinato alla conservazione permanente dei documenti aventi rilevanza giuridico-amministrativa.

I documenti soggetti a obblighi di protocollazione, archiviazione e conservazione a norma continuano pertanto a essere gestiti esclusivamente tramite il sistema Gecodoc e gli ulteriori sistemi conformi alle disposizioni vigenti.

Il rispetto della normativa sulla gestione documentale consente di garantire:

- la **corretta separazione dei sistemi e delle responsabilità**;
- la **validità giuridica degli atti amministrativi**;
- la **tracciabilità e la trasparenza** dell'azione amministrativa dell'Istituzione scolastica.

2.4 Principio DNSH (Do No Significant Harm): quadro normativo europeo

Il principio **DNSH – “Do No Significant Harm”** costituisce uno dei pilastri fondamentali del quadro normativo europeo che disciplina l'utilizzo delle risorse del **Piano Nazionale di Ripresa e Resilienza (PNRR)**, in attuazione del programma **Next Generation EU**.

Tale principio impone che ogni intervento finanziato con fondi europei **non arrechi danni significativi a nessuno degli obiettivi ambientali** individuati dalla normativa dell'Unione europea in materia di sostenibilità.

Il riferimento normativo principale è rappresentato dal **Regolamento (UE) 2020/852** (cosiddetto *Regolamento Tassonomia*), che definisce i criteri per determinare se un'attività economica possa considerarsi ecosostenibile. In particolare, il Regolamento individua sei obiettivi ambientali:

- mitigazione dei cambiamenti climatici;
- adattamento ai cambiamenti climatici;
- uso sostenibile e protezione delle risorse idriche e marine;
- transizione verso un'economia circolare;
- prevenzione e riduzione dell'inquinamento;
- protezione e ripristino della biodiversità e degli ecosistemi.

Ai fini del PNRR, il rispetto del principio DNSH è reso operativo attraverso specifici **atti di indirizzo e linee guida della Commissione europea e delle autorità nazionali competenti**, che richiedono alle amministrazioni beneficiarie dei finanziamenti di dimostrare che le attività realizzate:

- non comportano un incremento significativo delle emissioni climalteranti;

- non determinano un uso inefficiente o non sostenibile delle risorse naturali;
- non producono impatti ambientali negativi rilevanti, diretti o indiretti.

Nel contesto delle infrastrutture digitali e dei sistemi informatici, il principio DNSH si traduce, in particolare, nell'adozione di soluzioni tecnologiche che garantiscano:

- **efficienza energetica** dei data center e dei server utilizzati;
- utilizzo di infrastrutture conformi a standard ambientali riconosciuti;
- riduzione dei consumi energetici e delle risorse hardware;
- corretta gestione del ciclo di vita delle apparecchiature informatiche.

L'Istituzione scolastica, in qualità di soggetto beneficiario di fondi PNRR, è tenuta a **documentare e dimostrare il rispetto del principio DNSH** nell'adozione e nell'utilizzo del sistema documentale complementare, anche mediante la scelta di **server DNSH-compliant** e l'adozione di comportamenti organizzativi coerenti con gli obiettivi di sostenibilità ambientale.

Il rispetto del principio DNSH rappresenta pertanto un **requisito trasversale e vincolante**, che si affianca agli obblighi di conformità normativa, sicurezza e corretta gestione dei dati personali disciplinati dalle presenti Linee guida.

2.5 Altri standard e linee guida di riferimento

Oltre alla normativa europea e nazionale richiamata nei paragrafi precedenti, l'utilizzo del sistema documentale complementare da parte dell'Istituzione scolastica si ispira a ulteriori **standard, linee guida e buone pratiche**, che costituiscono riferimento per l'organizzazione, la sicurezza e la sostenibilità dei sistemi informativi della Pubblica Amministrazione.

In particolare, assumono rilievo:

- le **Linee guida dell'Agenzia per l'Italia Digitale (AgID)** in materia di sicurezza informatica, interoperabilità e gestione dei servizi digitali della Pubblica Amministrazione, nella misura in cui risultino applicabili al contesto scolastico;
- le **Linee guida e i provvedimenti dell'Autorità Garante per la protezione dei dati personali**, quali strumenti interpretativi e di indirizzo per la corretta applicazione della normativa in materia di dati personali, con particolare attenzione ai trattamenti effettuati da enti pubblici e al trattamento dei dati dei minori;
- il **Piano Triennale per l'Informatica nella Pubblica Amministrazione**, adottato a livello nazionale, che definisce le strategie e i principi per la digitalizzazione della PA, inclusi i temi della sicurezza, della sostenibilità e dell'efficienza delle infrastrutture digitali;
- gli **standard internazionali in materia di sicurezza delle informazioni**, quali le norme della famiglia ISO/IEC 27000, richiamati come buone pratiche di riferimento per l'adozione di misure organizzative e tecniche adeguate, pur in assenza di obblighi di

certificazione per l'Istituzione scolastica;

- le **linee guida e le indicazioni operative relative al PNRR**, emanate dalle amministrazioni centrali competenti, con particolare riferimento agli obblighi di rendicontazione, tracciabilità e rispetto del principio DNSH.

Tali riferimenti contribuiscono a delineare un **quadro coerente di regole e buone pratiche**, volto a garantire che l'utilizzo del sistema documentale complementare:

- sia conforme ai principi di legalità, trasparenza e responsabilizzazione;
- avvenga in condizioni di adeguata sicurezza e protezione dei dati personali;
- sia coerente con gli obiettivi di sostenibilità ambientale e di innovazione digitale promossi dall'Unione europea e dal PNRR.

In particolare l'Istituto è obbligato ad utilizzare solo soluzioni certificate dall'Agenzia per la Cybersicurezza Nazionale (ACN)

Le presenti Linee guida recepiscono tali standard e indicazioni come **riferimenti interpretativi e operativi**, fermo restando il rispetto delle disposizioni normative vincolanti e delle specificità organizzative dell'Istituzione scolastica.

3 – Descrizione del sistema documentale

3.1 Caratteristiche generali del sistema

Il sistema documentale complementare adottato dall'Istituzione scolastica è una **piattaforma digitale per la gestione e la condivisione di documenti informatici o comunque di documenti digitali** (ossia file non contenenti rappresentazioni di dati non giuridicamente rilevanti), progettata per supportare le attività amministrative e didattiche dell'Istituto, in integrazione con i sistemi istituzionali già in uso.

Questo sistema può ospitare anche la documentazione predisposta dai Comitati Genitori nell'ambito della loro attività istituzionale, previa autorizzazione da parte dell'Istituto comprensivo.

Il sistema si configura come **strumento di collaborazione e organizzazione documentale**, con le seguenti caratteristiche generali:

- **accesso esclusivo tramite identità digitale** (SPID/CIE/eIDAS) e profili autorizzativi differenziati;
- gestione centralizzata dei documenti informatici;
- possibilità di condivisione controllata dei documenti tra utenti autorizzati;
- tracciabilità delle operazioni di caricamento, modifica e consultazione;
- utilizzo tramite infrastruttura server conforme ai requisiti DNSH.

Il sistema documentale complementare è destinato a facilitare:

- la circolazione interna delle informazioni;
- il lavoro collaborativo tra personale scolastico;
- la condivisione di materiali didattici e documentazione organizzativa anche rivolta alle famiglie;
- il supporto ai progetti e alle attività della scuola.

3.2 Assenza di funzionalità di Intelligenza Artificiale

Il sistema documentale complementare **non utilizza né integra funzionalità di Intelligenza Artificiale**, né algoritmi di apprendimento automatico o sistemi di profilazione automatizzata degli utenti, salvo chatbot descrittive delle funzionalità del sistema senza accesso ai dati archiviati.

In particolare:

- non vengono effettuate analisi automatizzate dei contenuti dei documenti;

- non sono presenti sistemi di classificazione, indicizzazione o valutazione basati su IA;
- non vengono adottati processi decisionali automatizzati ai sensi della normativa europea in materia di protezione dei dati personali.

I trattamenti di dati personali avvengono esclusivamente mediante **operazioni manuali o automatizzazioni tecniche di base**, necessarie al funzionamento del sistema, sotto il controllo degli utenti autorizzati e nel rispetto delle presenti Linee guida.

E' previsto lo sviluppo progressivo di un'API (Application Program Interface) per il sistema documentale complementare Pluridoc, ai fini dell'automazione dei processi di profilatura e attribuzione dei privilegi agli utenti, ma senza funzionalità controllate dall'IA.

3.3 Tipologia di documenti trattati

Attraverso il sistema documentale complementare possono essere gestiti e condivisi, a titolo esemplificativo e non esaustivo:

- documenti amministrativi interni non soggetti a protocollazione;
- documentazione organizzativa e di servizio, anche a supporto degli organi collegiali (Consiglio d'Istituto, Collegio dei Docenti);
- materiali didattici e contenuti a supporto delle attività educative;
- documentazione relativa a progetti, iniziative e attività scolastiche, anche prodotti dal Comitato Genitori;
- documenti di lavoro e bozze non aventi rilevanza giuridico-amministrativa.

I documenti possono contenere **dati personali**, inclusi dati relativi a studenti, famiglie, personale docente e personale ATA, esclusivamente nei limiti delle finalità istituzionali e delle autorizzazioni assegnate.

Restano esclusi dal sistema documentale complementare i documenti soggetti a **protocollo informatico, archiviazione e conservazione digitale a norma**, che devono essere gestiti esclusivamente tramite i sistemi istituzionali preposti.

3.4 Ciclo di vita del documento

Il ciclo di vita dei documenti gestiti nel sistema documentale complementare comprende le seguenti fasi:

- **creazione o caricamento** del documento da parte di un utente autorizzato;
- **condivisione** del documento con altri utenti o gruppi, secondo i profili di accesso assegnati;

- **utilizzo e consultazione** del documento per le finalità amministrative o didattiche previste;
- **aggiornamento o modifica**, se consentito dalle autorizzazioni;
- **archiviazione temporanea o cancellazione**, in conformità alle regole interne e ai tempi di conservazione definiti e nel rispetto delle regole del GDPR. Per ogni documento deve essere indicata la data di rimozione dalla visualizzazione, nel rispetto del diritto all'oblio.

Il sistema è progettato per garantire che ogni fase del ciclo di vita del documento avvenga nel rispetto dei principi di **sicurezza, riservatezza, minimizzazione dei dati e tracciabilità delle operazioni**, come richiesto dalla normativa vigente e dalle presenti Linee guida.

3.5 Canali di distribuzione nel sistema documentale complementare

Il sistema documentale adottato nella scuola è basato su un modello di **spazi di lavoro indipendenti**, definiti come **canali**, che costituiscono l'elemento principale di organizzazione, condivisione e accesso ai documenti.

I **canali** rappresentano aree tematiche oppure funzionali all'interno del sistema e consentono di raggruppare documenti e contenuti in maniera strutturata, assegnando **permessi di accesso differenziati agli utenti autorizzati**.

Dal punto di vista funzionale, i canali possono essere configurati secondo diverse modalità di accesso e distribuzione delle informazioni:

1. Canali privati

I canali privati sono accessibili **soltanto a utenti autenticati** e in possesso di credenziali abilitate al sistema documentale. L'accesso ai documenti all'interno di un canale privato avviene dopo autenticazione e assegnazione di specifici **permessi di visualizzazione e modifica**. Questo tipo di canale è utilizzato per la gestione e la condivisione di documenti riservati, contenenti dati personali o informazioni sensibili, nel rispetto dei principi di sicurezza e riservatezza previsti dalla normativa sulla protezione dei dati personali.

2. Canali pubblici

I canali pubblici consentono l'accesso ai documenti **senza autenticazione**, attraverso un indirizzo web pubblico oppure tramite link aperto. Questo tipo di canale può essere utilizzato per la condivisione di documenti non riservati a un pubblico più ampio, ad esempio materiali informativi generali, indicatori di progetto, linee guida non soggette a riservatezza oppure comunicazioni destinate a utenti esterni alla scuola. La configurazione di canali pubblici è possibile soltanto a seguito di **specifica valutazione di opportunità e conformità normativa**, in particolare con riferimento alla tutela dei dati personali e alla sicurezza delle informazioni.

I canali pubblici costituiscono l'unico canale utilizzabile per la condivisione e la diffusione di materiale divulgativo e promozionale sulle attività dell'Istituto. Non è consentito l'utilizzo di piattaforme di social media.

3. Canali ibridi

I canali ibridi combinano elementi delle due configurazioni precedenti: l'accesso al canale richiede autenticazione, ma alcuni documenti all'interno del canale possono essere resi accessibili anche tramite **link pubblico**, senza autenticazione. Tale modalità deve essere utilizzata con cautela e sempre nel rispetto delle regole di protezione dei dati e di sicurezza dell'Istituto scolastico, garantendo che nessun dato personale sensibile sia esposto senza adeguata protezione.

La scelta del tipo di canale è funzione delle **finalità di utilizzo** e dei **livelli di protezione richiesti** per i documenti condivisi, con particolare attenzione alle categorie di dati trattati e alla loro riservatezza. L'adozione di una tipologia piuttosto che un'altra deve essere coerente con i principi di minimizzazione dei dati, riservatezza e sicurezza, così come richiesto dalla normativa europea sulla protezione dei dati personali.

4.1 Localizzazione e caratteristiche dei server

Il sistema documentale complementare adottato dall'Istituzione scolastica deve essere ospitato su infrastruttura server all'interno del territorio dell'Unione Europea e deve rispettare i requisiti di sicurezza e rispetto dell'ambiente.

In particolare l'istanza di Pluridoc realizzata grazie ai finanziamenti PNRR è installata su OVHcloud e collocata presso data center situati nel territorio dell'Unione europea.

La localizzazione dei server all'interno dell'UE garantisce che:

- il trattamento dei dati personali avvenga in un contesto normativo conforme alla **legislazione europea in materia di protezione dei dati personali**;
- siano applicabili le disposizioni del Regolamento (UE) 2016/679 (GDPR) senza necessità di ricorrere a meccanismi di trasferimento verso Paesi terzi;
- siano assicurati adeguati livelli di tutela giuridica, tecnica e organizzativa per i dati trattati.

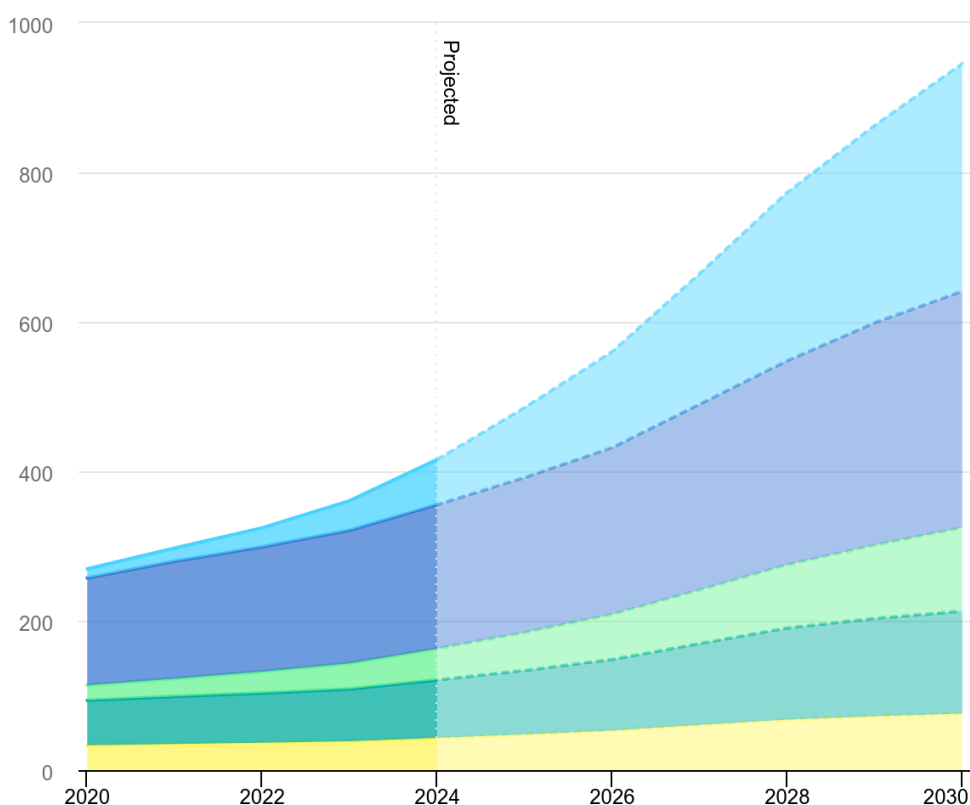
I server utilizzati per l'erogazione del sistema documentale presentano le seguenti caratteristiche generali:

- infrastruttura di tipo **data center professionale**, con elevati standard di affidabilità e continuità del servizio;
- adozione di **misure di sicurezza fisica e logica** per la protezione dei dati e dei sistemi;
- utilizzo di tecnologie orientate all'**efficienza energetica** e alla riduzione dell'impatto ambientale;
- conformità ai requisiti richiesti dal principio **DNSH (Do No Significant Harm)**, in coerenza con gli obiettivi ambientali previsti dal quadro normativo europeo e dal PNRR.

In particolare i data center utilizzati sono certificati ISO 14001 e rispettano i criteri del [Code of Conduct for Energy Efficiency in Data Centers](#) della Commissione Europea.

I data center sono infrastrutture complesse che, per fornire servizi digitali 24 ore su 24, **richiedono quantità significative di energia elettrica**. Per comprendere l'impatto energetico di questi sistemi, è utile considerare alcuni dati di riferimento a livello globale ed europeo¹:

- **Consumo globale:** secondo stime dell'Agenzia Internazionale dell'Energia (IEA), nel 2024 i data center nel mondo hanno consumato circa **415 terawattora (TWh)** di elettricità, pari a circa **1,5 % del consumo elettrico mondiale** (approssimativamente 30.000 TWh):



Global data centre electricity consumption, by equipment, Base Case, 2020-2030
(in ordinata l'energia consumata in TWh)

Fonte:

<https://www.iea.org/data-and-statistics/charts/global-data-centre-electricity-consumption-by-equipment-base-case-2020-2030>

- **Trend di crescita:** se non contenuti da misure di efficienza, i consumi globali potrebbero **raddoppiare entro il 2030**, raggiungendo circa **945 TWh**, con i data center che arriverebbero a rappresentare quasi **3 % del consumo mondiale di elettricità**.

1

https://energy.ec.europa.eu/news/focus-data-centres-energy-hungry-challenge-2025-11-17_en#:~:text=Accor ding%20to%20the%20International%20Energy,towards%20115%20TWh%20by%202030.

- **Situazione europea:** nell'Unione Europea i consumi dei data center sono stimati a **circa 70 TWh all'anno**, pari a circa il **2 % della domanda elettrica totale europea** nel 2024.
- **Efficienza energetica e PUE:** il parametro **PUE (Power Usage Effectiveness)**, utilizzato per misurare l'efficienza energetica di un data center, indica quanta parte dell'energia totale consumata è effettivamente utilizzata per far funzionare l'equipaggiamento informatico. Un valore ideale è **1,0**; valori più alti indicano consumi maggiori per raffreddamento e servizi ausiliari. Il valore medio mondiale si aggira intorno a **1,8**. I server scelti dall'Istituto scolastico hanno valori PUE attorno a 1,2 (https://www.ovhcloud.com/sites/default/files/external_files/kpis_per_dc-fy24.pdf?_gl=1*m5zqf5*_gcl_au*MTA5NDkxMTQxNS4xNzcxMDg2MjI1)

Per fornire un contesto comparativo, l'energia consumata annualmente da data center a livello globale è paragonabile, in ordine di grandezza, al consumo elettrico di **interi Paesi di medie dimensioni**.

Questi dati numerici aiutano a comprendere perché l'efficienza energetica dei data center sia un tema cruciale nelle strategie di sostenibilità ambientale e perché iniziative come il **Code of Conduct for Energy Efficiency in Data Centers** siano parte integrante del quadro di riferimento per il rispetto del principio **DNSH (Do No Significant Harm)** e degli obiettivi PNRR.

La scelta di una infrastruttura server localizzata presso i data center certificati secondo criteri DNSH risulta coerente con:

- le esigenze di **affidabilità e sicurezza** del servizio documentale;
- gli obblighi di **protezione dei dati personali**, con particolare riferimento ai dati di studenti e minori;
- i requisiti di **sostenibilità ambientale** richiesti per i progetti finanziati con risorse PNRR.

L'Istituzione scolastica mantiene in ogni caso la responsabilità del corretto utilizzo del sistema documentale e del rispetto delle presenti Linee guida, fermo restando che l'infrastruttura tecnologica di hosting costituisce elemento essenziale per garantire la conformità normativa e ambientale dell'intera soluzione adottata.

4.3 Efficienza energetica e sostenibilità ambientale

L'efficienza energetica e la sostenibilità ambientale costituiscono elementi centrali nella progettazione e nell'utilizzo del sistema documentale complementare adottato dall'Istituzione scolastica, in coerenza con il principio **DNSH (Do No Significant Harm)** e con gli obiettivi ambientali del **PNRR**.

In particolare, l'adozione di un sistema documentale basato su **infrastruttura server professionale** consente di concentrare l'erogazione dei servizi digitali in ambienti tecnologici progettati per:

- ottimizzare i consumi energetici complessivi;
- ridurre le dispersioni di energia legate al raffreddamento e all'alimentazione;
- migliorare il rapporto tra energia consumata e capacità di calcolo effettivamente utilizzata.

Dal punto di vista ambientale, l'efficienza energetica dei data center si traduce in una **riduzione indiretta delle emissioni climalteranti**, in quanto una minore richiesta di energia elettrica comporta, a parità di mix energetico, un minore impatto sull'ambiente.

L'utilizzo di un'infrastruttura centralizzata ed efficiente risulta inoltre preferibile rispetto a soluzioni frammentate o locali, che comporterebbero:

- maggiore duplicazione di hardware;
- minore controllo sui consumi energetici;
- difficoltà di monitoraggio e ottimizzazione delle risorse.

Nel contesto delle presenti Linee guida, la sostenibilità ambientale è perseguita attraverso:

- la scelta di **infrastrutture server DNSH-compliant**, orientate all'efficienza energetica;
- l'allineamento alle **migliori pratiche europee** in materia di gestione dei data center, incluse quelle previste dal *Code of Conduct for Energy Efficiency in Data Centers*;
- l'utilizzo consapevole del sistema documentale da parte degli utenti, evitando carichi ridondanti, duplicazioni non necessarie di documenti e conservazioni superflue.

L'Istituzione scolastica contribuisce così, nell'ambito delle proprie competenze e dimensioni organizzative, al raggiungimento degli obiettivi di **transizione digitale sostenibile**, promuovendo un uso responsabile delle tecnologie informatiche e dimostrando coerenza tra innovazione digitale e tutela ambientale.

L'efficienza energetica e la sostenibilità ambientale non sono pertanto considerate aspetti esclusivamente tecnici, ma **principi trasversali** che orientano le scelte organizzative e operative legate all'utilizzo del sistema documentale complementare.

4.4 Misure di riduzione dell'impatto ambientale

Nel rispetto del principio **DNSH (Do No Significant Harm)** e degli obiettivi di sostenibilità ambientale previsti dal **PNRR**, l'Istituzione scolastica adotta e promuove una serie di **misure organizzative e operative** finalizzate alla riduzione dell'impatto ambientale connesso all'utilizzo del sistema documentale complementare.

Tali misure si collocano su più livelli, tenendo conto del fatto che l'Istituzione scolastica **non gestisce direttamente l'infrastruttura hardware**, ma ne utilizza i servizi tramite fornitori specializzati.

In particolare, sono adottate le seguenti misure:

- **selezione di infrastrutture di hosting DNSH-compliant**, localizzate all'interno dell'Unione europea e orientate all'efficienza energetica e alla sostenibilità ambientale;
- **centralizzazione della gestione documentale**, che consente di ridurre la duplicazione di sistemi locali, dispositivi di archiviazione fisica e supporti cartacei;
- **riduzione dell'uso di carta**, attraverso la condivisione digitale dei documenti e l'adozione di flussi documentali informatizzati per le attività amministrative e didattiche;
- **limitazione delle duplicazioni non necessarie di documenti**, favorendo l'accesso condiviso ai contenuti piuttosto che la creazione di copie multiple;
- **gestione consapevole dei tempi di conservazione**, evitando l'accumulo di documenti non più necessari e riducendo l'occupazione di spazio di archiviazione;
- **sensibilizzazione degli utenti autorizzati** all'utilizzo responsabile del sistema documentale, anche in termini di sostenibilità ambientale e consumo delle risorse digitali.

L'Istituzione scolastica promuove inoltre comportamenti coerenti con i principi di sostenibilità, quali:

- l'adozione di modalità di lavoro collaborative digitali;
- l'utilizzo di strumenti informatici condivisi;
- la razionalizzazione delle attività di archiviazione e gestione dei documenti.

L'insieme di tali misure contribuisce a **ridurre l'impatto ambientale complessivo** delle attività amministrative e didattiche svolte tramite il sistema documentale, in coerenza con gli obiettivi europei di transizione ecologica e con gli obblighi di responsabilizzazione richiesti per i progetti finanziati con risorse PNRR.

5 – Principi di protezione dei dati personali

Introduzione

Il sistema documentale complementare adottato dall'Istituzione scolastica comporta il **trattamento di dati personali**, in quanto consente la creazione, la condivisione e la consultazione di documenti che possono contenere informazioni riferite a persone fisiche identificabili, quali studenti, famiglie, personale docente e personale ATA.

La protezione dei dati personali rappresenta pertanto un **obbligo giuridico** e un **dovere organizzativo** per la scuola, che opera come soggetto pubblico nell'ambito delle proprie funzioni istituzionali. Ogni utilizzo del sistema documentale deve avvenire nel rispetto dei principi stabiliti dalla normativa europea e nazionale in materia di protezione dei dati personali.

Il **Regolamento (UE) 2016/679 (GDPR)** individua una serie di **principi fondamentali** che devono guidare qualsiasi trattamento di dati personali, indipendentemente dagli strumenti tecnologici utilizzati. Tali principi costituiscono la base di riferimento anche per l'uso del sistema documentale complementare disciplinato dalle presenti Linee guida.

Questa Sezione ha lo scopo di:

- illustrare in modo **semplice e comprensibile** i principali principi di protezione dei dati personali;
- chiarire come tali principi si applicano, in concreto, all'utilizzo del sistema documentale complementare;
- fornire agli utenti autorizzati indicazioni di comportamento utili a prevenire utilizzi impropri o non conformi dei dati personali.

I paragrafi che seguono descrivono ciascun principio in forma esplicita evidenziandone il significato essenziale e la rilevanza pratica per le attività amministrative e didattiche della scuola.

5.1 Liceità, correttezza e trasparenza

I dati personali devono essere trattati solo quando esiste una **base giuridica legittima**, nel rispetto delle funzioni istituzionali della scuola e in modo corretto nei confronti degli interessati. L'utilizzo del sistema documentale deve avvenire in modo **chiaro e comprensibile**, evitando trattamenti nascosti o non dichiarati e garantendo che studenti, famiglie e personale siano adeguatamente informati.

5.2 Limitazione delle finalità

I dati personali devono essere raccolti e utilizzati **esclusivamente per finalità determinate e legittime**, connesse alle attività amministrative e didattiche della scuola.

I documenti condivisi nel sistema non possono essere riutilizzati per scopi diversi o incompatibili rispetto a quelli per cui sono stati originariamente creati.

5.3 Minimizzazione dei dati

Devono essere trattati **solo i dati strettamente necessari** per il raggiungimento delle finalità previste.

Nel sistema documentale non devono essere caricati documenti contenenti informazioni eccedenti, superflue o non pertinenti rispetto all'attività svolta.

5.4 Esattezza dei dati

I dati personali devono essere **corretti e aggiornati**.

Gli utenti autorizzati sono tenuti a verificare, per quanto di competenza, l'accuratezza delle informazioni contenute nei documenti condivisi e a segnalare o correggere eventuali errori.

5.5 Limitazione della conservazione

I dati personali devono essere conservati **per un periodo di tempo non superiore a quello necessario** alle finalità per cui sono trattati.

Nel sistema documentale complementare i documenti devono essere eliminati o archiviati quando non risultano più utili, nel rispetto delle regole interne e della distinzione rispetto alla conservazione a norma.

5.6 Integrità e riservatezza

I dati personali devono essere protetti da **accessi non autorizzati, divulgazioni indebite, perdite o distruzioni accidentali**.

Ogni utente è responsabile dell'uso corretto delle proprie credenziali e del rispetto dei livelli di accesso assegnati, evitando la condivisione impropria dei documenti.

5.7 Responsabilizzazione (Accountability)

Il titolare del trattamento deve essere in grado di **dimostrare il rispetto della normativa** in materia di protezione dei dati personali.

Ciò implica l'adozione di regole interne, la definizione di ruoli e responsabilità e il rispetto delle presenti Linee guida da parte di tutti gli utenti autorizzati.

6 – Ruoli e responsabilità

La corretta gestione del sistema documentale complementare richiede una **chiara definizione dei ruoli e delle responsabilità**, al fine di garantire il rispetto della normativa in materia di protezione dei dati personali, della sicurezza delle informazioni e delle presenti Linee guida.

Ogni soggetto coinvolto è tenuto a operare **nei limiti delle funzioni attribuite** e delle autorizzazioni assegnate.

6.1 Titolare del trattamento

Il **Titolare del trattamento** è l'Istituzione scolastica, nella persona del **Dirigente scolastico**. Il Titolare determina le finalità e i mezzi del trattamento dei dati personali e assicura che il sistema documentale sia utilizzato nel rispetto della normativa vigente e delle presenti Linee guida.

6.2 Responsabili del trattamento

I **Responsabili del trattamento** sono i soggetti esterni che forniscono servizi connessi al sistema documentale, operando per conto della scuola. Per il sistema complementare Pluridoc il responsabile del trattamento è il produttore e gestore del software.

Essi trattano i dati personali esclusivamente sulla base di istruzioni documentate del Titolare e nel rispetto delle misure di sicurezza previste dalla normativa.

6.3 Amministratori di sistema

Gli **Amministratori di sistema** sono incaricati della gestione tecnica e operativa del sistema documentale.

Essi operano sulla base di specifiche autorizzazioni, garantendo la sicurezza, la disponibilità del servizio e il corretto funzionamento della piattaforma, senza accedere ai contenuti dei documenti se non strettamente necessario per finalità tecniche.

6.4 Utenti autorizzati

Gli **utenti autorizzati** comprendono il personale docente, il personale amministrativo, tecnico e ATA e gli altri soggetti interni formalmente abilitati.

Ogni utente può accedere al sistema documentale solo nei limiti del **profilo assegnato** ed è responsabile del corretto utilizzo dei documenti e dei dati personali trattati.

6.5 Responsabili dei Comitati Genitori

I **Responsabili dei Comitati Genitori** possono essere autorizzati all'accesso al sistema documentale complementare **esclusivamente previa formale autorizzazione del Dirigente scolastico**.

L'accesso è limitato ai documenti strettamente necessari allo svolgimento delle attività e delle iniziative di competenza dei Comitati e avviene nel rispetto dei principi di riservatezza e minimizzazione dei dati.

6.6 Obblighi di riservatezza e formazione

Tutti i soggetti autorizzati all'utilizzo del sistema documentale sono tenuti a:

- rispettare gli **obblighi di riservatezza** sui dati e sulle informazioni trattate;
- utilizzare il sistema esclusivamente per finalità istituzionali;
- attenersi alle presenti Linee guida e alle istruzioni ricevute;
- partecipare, ove previsto, alle attività di **informazione e formazione** in materia di protezione dei dati personali e sicurezza informatica.

Il mancato rispetto dei ruoli e delle responsabilità assegnate può comportare conseguenze di natura organizzativa e disciplinare o il mancato rispetto della *compliance* normativa.

7 – Sicurezza del sistema documentale

La sicurezza del sistema documentale complementare è un elemento fondamentale per tutelare la riservatezza, l'integrità e la disponibilità delle informazioni condivise. Il sistema adottato supporta **meccanismi di controllo degli accessi, autenticazione, gestione dei permessi e monitoraggio delle attività**, in linea con gli obblighi normativi di protezione dei dati personali.

7.1 Controllo degli accessi e autenticazione

L'accesso al sistema documentale avviene tramite **autenticazione con sistemi di autenticazione avanzati (SPID/CIE/eIDAS)**, garantendo che solo gli utenti autorizzati possano visualizzare o gestire i documenti contenuti nei canali privati o ibridi.

La piattaforma assegna accessi diversi secondo la tipologia di canale (privato, pubblico, ibrido) e i profili utente: *Admin, Uploader, Uploader Light e Viewer*, ciascuno con responsabilità e permessi specifici.

7.2 Gestione dei permessi

La sicurezza è assicurata anche tramite un sistema di **permessi granulare**, in cui è possibile definire quali utenti possono:

- visualizzare documenti specifici;
- caricarli o modificarli;
- gestire cartelle o l'intero canale.

Questi livelli di permesso riducono il rischio di accessi non autorizzati e assicurano che gli utenti possano operare solo entro lo **scopo funzionale a loro assegnato**.

7.3 Monitoraggio e registrazione delle attività

Il sistema documentale prevede un **monitoraggio delle attività degli utenti**, consentendo di tracciare:

- chi ha effettuato l'accesso;
- quali documenti sono stati visualizzati, caricati, modificati o scaricati;

- quando tali operazioni sono state eseguite.

Tali informazioni consentono di verificare la correttezza dei trattamenti effettuati e costituiscono elemento utile per eventuali attività di controllo, audit e rendicontazione.

7.4 Sicurezza logica delle informazioni

Il sistema adotta **misure tecniche di sicurezza logica**, come la protezione delle credenziali, la cifratura dei dati in transito e una struttura di permessi che limita l'accesso ai documenti sensibili.

In contesti in cui è previsto l'uso di canali ibridi o pubblici, la condivisione di link deve essere sempre valutata con attenzione e nel rispetto delle regole di protezione dei dati.

7.5 Gestione delle vulnerabilità e aggiornamenti

Il fornitore della piattaforma mantiene aggiornati i componenti software e le funzionalità, per ridurre il rischio di vulnerabilità note e per allinearsi alle migliori pratiche di sicurezza.

La scuola, dal canto suo, promuove un uso corretto e responsabile dello strumento, segnalando eventuali anomalie o sospetti di violazione ai responsabili tecnici e al Titolare del trattamento.

7.6 Ruolo degli amministratori di sistema

Gli **Amministratori di sistema** sono incaricati di:

- attivare e disattivare utenze;
- assegnare e revocare ruoli;
- gestire la configurazione dei canali;
- monitorare i log delle attività.

La loro azione si svolge nel rispetto delle disposizioni di riservatezza e delle autorizzazioni attribuite, senza accedere ai contenuti dei documenti se non per esigenze tecniche strettamente necessarie.

7.7 Gestione delle violazioni dei dati personali (Data Breach)

Per **violazione dei dati personali (data breach)** si intende qualsiasi evento che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati tramite il sistema documentale.

In caso di sospetta o accertata violazione dei dati personali:

- l'evento deve essere **tempestivamente segnalato** al Dirigente scolastico o ai soggetti da lui individuati;
- devono essere attivate le procedure interne per la **valutazione dell'impatto** della violazione sui diritti e sulle libertà degli interessati;
- ove necessario, il Titolare del trattamento provvede alla **notifica all'Autorità Garante per la protezione dei dati personali** nei termini previsti dalla normativa;
- nei casi più gravi, può essere richiesta anche la **comunicazione agli interessati**, secondo le modalità previste dal GDPR.

Il sistema documentale, grazie ai meccanismi di tracciamento delle attività e di controllo degli accessi, consente di **ricostruire gli eventi** e supportare le attività di analisi e gestione dell'incidente.

Tutti gli utenti autorizzati sono tenuti a:

- adottare comportamenti prudenti nell'uso del sistema;
- proteggere le proprie credenziali di accesso SPID/CIE/eIDAS;
- segnalare immediatamente eventuali anomalie, accessi sospetti o errori che possano compromettere la sicurezza dei dati.

La corretta gestione delle violazioni dei dati personali costituisce parte integrante degli obblighi di **sicurezza, responsabilizzazione e tutela degli interessati**, ed è essenziale per garantire la conformità normativa e la fiducia nell'utilizzo del sistema documentale.

8 – Gestione documentale e conformità normativa

La presente Sezione disciplina le modalità di utilizzo del sistema documentale complementare in relazione alla **gestione dei documenti informatici**, nel rispetto della normativa vigente e delle disposizioni interne dell'Istituzione scolastica.

8.1 Classificazione e organizzazione dei documenti

I documenti caricati nel sistema documentale complementare devono essere **organizzati in modo ordinato e coerente**, utilizzando strutture di cartelle, canali o spazi di lavoro definiti in base alle attività amministrative e didattiche.

Una corretta organizzazione facilita la consultazione, riduce il rischio di duplicazioni e contribuisce alla sicurezza e alla corretta gestione delle informazioni.

8.2 Regole di utilizzo del sistema documentale complementare

Il sistema documentale complementare deve essere utilizzato esclusivamente per **finalità istituzionali**, amministrative e didattiche.

È vietato l'utilizzo del sistema per scopi personali o estranei alle attività della scuola. Ogni utente è responsabile dei documenti caricati e condivisi nel rispetto delle autorizzazioni assegnate.

8.3 Distinzione tra documenti gestionali e documenti soggetti a protocollo

Nel sistema documentale complementare possono essere gestiti **documenti di lavoro, materiali didattici, documentazione organizzativa e bozze o documentazione delle attività didattiche**, anche a cura (previa autorizzazione dell'Istituto) del Comitato Genitori.

I documenti soggetti a **protocollo informatico, archiviazione e conservazione a norma** devono essere gestiti esclusivamente tramite i sistemi istituzionali preposti e **non devono essere conservati nel sistema documentale complementare** se non come copie di lavoro temporanee.

8.4 Conservazione dei documenti e tempi di permanenza nel sistema

I documenti devono essere conservati nel sistema documentale **solo per il tempo necessario** al raggiungimento delle finalità per cui sono stati caricati.

Una volta esaurita la funzione operativa o didattica, i documenti devono essere cancellati o trasferiti ai sistemi competenti, nel rispetto delle regole interne e della normativa applicabile.

Il sistema documentale complementare assicura che all'atto del caricamento di ogni documento debba essere inserita la data di rimozione dalla visualizzazione, in conformità al c.d. diritto all'oblio.

8.5 Integrità, immutabilità e reperibilità dei documenti

Il sistema documentale garantisce l'integrità dei documenti durante il periodo di utilizzo.

Gli utenti devono evitare modifiche non autorizzate, versioni parallele non controllate o cancellazioni improprie, assicurando che i documenti restino **reperibili, leggibili e coerenti** con le finalità di utilizzo.

8.6 Procedure di backup e ripristino

Il sistema documentale è supportato da **procedure di backup** gestite a livello infrastrutturale dal fornitore del servizio.

Tali procedure consentono il ripristino dei dati in caso di malfunzionamenti o incidenti tecnici, contribuendo alla continuità operativa del servizio.

8.7 Cancellazione e dismissione dei documenti

La cancellazione dei documenti dal sistema documentale deve avvenire in modo **consapevole e controllato**, evitando eliminazioni accidentali o premature.

La dismissione dei documenti contribuisce alla **riduzione dei rischi di trattamento non necessario dei dati personali** e al contenimento dell'impatto ambientale legato all'archiviazione digitale.

10 – Diritti degli interessati

Il trattamento dei dati personali effettuato tramite il sistema documentale complementare deve garantire il pieno rispetto dei **diritti riconosciuti agli interessati** dalla normativa europea e nazionale in materia di protezione dei dati personali.

Per *interessati* si intendono, in particolare, studenti, famiglie, personale docente, personale ATA e ogni altra persona fisica i cui dati siano trattati nell'ambito delle attività della scuola.

10.1 Diritti riconosciuti dalla normativa

Gli interessati hanno il diritto di:

- ottenere informazioni sul trattamento dei propri dati personali;
- accedere ai dati che li riguardano;
- richiedere la rettifica dei dati inesatti o incompleti;
- richiedere, nei casi previsti, la cancellazione o la limitazione del trattamento;
- opporsi al trattamento, nei limiti consentiti dalla normativa.

Tali diritti sono esercitabili nel rispetto delle funzioni istituzionali della scuola e delle disposizioni normative applicabili ai soggetti pubblici.

10.2 Modalità di esercizio dei diritti

Le richieste di esercizio dei diritti devono essere presentate all'Istituzione scolastica secondo le modalità indicate nelle informative sul trattamento dei dati personali, disponibili al link <https://iccarvico.edu.it/informativa-privacy>

La scuola fornisce riscontro alle richieste nei **termini previsti dalla normativa**, adottando procedure interne idonee a garantire correttezza, tracciabilità e tempestività.

10.3 Limiti all'esercizio dei diritti

L'esercizio dei diritti può essere limitato nei casi previsti dalla legge, in particolare quando il trattamento è necessario per l'adempimento di obblighi legali o per l'esecuzione di compiti di interesse pubblico attribuiti all'Istituzione scolastica.

Il rispetto dei diritti degli interessati rappresenta un elemento essenziale per garantire **trasparenza, fiducia e correttezza** nell'utilizzo del sistema documentale complementare.

11 – Audit, controlli e aggiornamento delle Linee guida

La presente Sezione disciplina le attività di **verifica, controllo e aggiornamento** delle Linee guida, al fine di garantirne l'efficacia nel tempo e la conformità alla normativa vigente.

11.1 Attività di audit interni

L'Istituzione scolastica può effettuare **verifiche interne periodiche** sull'utilizzo del sistema documentale complementare, con l'obiettivo di:

- controllare il rispetto delle presenti Linee guida;
- verificare la corretta applicazione delle regole di sicurezza e protezione dei dati personali;
- individuare eventuali criticità organizzative o operative.

Le attività di audit possono essere svolte dal Dirigente scolastico o da soggetti da lui incaricati.

11.2 Controlli e tracciabilità

I controlli si avvalgono anche degli strumenti di **tracciamento delle attività** messi a disposizione dal sistema documentale, nel rispetto della normativa sulla protezione dei dati personali.

La tracciabilità consente di supportare le attività di controllo, prevenire utilizzi impropri e garantire la responsabilizzazione degli utenti autorizzati.

11.3 Aggiornamento delle Linee guida

Le presenti Linee guida sono soggette ad **aggiornamento periodico**, in particolare in caso di:

- modifiche normative o regolamentari;
- aggiornamenti significativi del sistema documentale o dell'infrastruttura tecnologica;
- nuove indicazioni relative al principio DNSH;
- esiti di audit o controlli che rendano necessario un adeguamento delle disposizioni interne.

Gli aggiornamenti sono approvati con le modalità previste dall'organizzazione interna dell'Istituzione scolastica e portati a conoscenza degli utenti interessati.

Disposizioni finali

Le presenti **Linee guida interne sull'utilizzo del sistema documentale complementare** costituiscono parte integrante delle disposizioni organizzative dell'Istituzione scolastica e sono vincolanti per tutti i soggetti autorizzati all'accesso e all'utilizzo del sistema.

12.1 Entrata in vigore

Le Linee guida entrano in vigore quindici giorni dopo la loro pubblicazione all'albo online dell'Istituzione scolastica, previa approvazione da parte del Consiglio d'Istituto, e si applicano a tutte le attività svolte mediante il sistema documentale complementare a partire da tale data.

12.2 Diffusione e conoscibilità

Il documento è reso disponibile al personale scolastico e agli altri soggetti autorizzati mediante i canali di comunicazione istituzionali della scuola.

La conoscenza e il rispetto delle Linee guida costituiscono condizione essenziale per l'utilizzo del sistema documentale complementare.

12.3 Responsabilità e conseguenze in caso di inosservanza

Il mancato rispetto delle presenti Linee guida può comportare l'adozione di misure organizzative e disciplinari, nel rispetto della normativa vigente e dei contratti applicabili, nonché eventuali conseguenze in relazione alla protezione dei dati personali.

12.4 Rinvio normativo

Per quanto non espressamente disciplinato dal presente documento, si rinvia alla normativa europea e nazionale vigente, alle disposizioni interne dell'Istituzione scolastica e alle linee guida emanate dalle autorità competenti.