Ministero dell'Istruzione e del Merito
Dipartimento per l'Istruzione
Direzione Generale per gli Affari Internazionali
Uff. V

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE
CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

DOCUMENTO DI POLICY E-SECURITY

Documento parte integrante del Regolamento di Istituto con Regolamento di Disciplina
Allegato al PTOF triennio 2025/2028
Delibera Collegio dei Docenti n. 45 del 10/11/2025.
Delibera Consiglio di Istituto n. 192 dell'11/11/2025.

Via Cerundolo, 64 – San Cesario di Lecce Tel.0832/205333
C.M. LEIC853003 – C.F. 80012820751
E-mail: leic853003@istruzione.it PEC: leic853003@pec.istruzione.it
www.comprensivosancesario.edu.it

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

PREMESSA
RIFERIMENTI AL PROGETTO GENERAZIONI CONNESSE
RIFERIMENTI NORMATIVI
CAPITOLO 1: INTRODUZIONE
1.1 SCOPO DELLA POLICY
1.2 AREE DI RISCHIO NELL'USO DELLE TECNOLOGIE DIGITALI
1.3 DISPOSIZIONI, COMPORTAMENTI E PROCEDURE PER L'USO SICURO DELLE TECNOLOGIE DIGITALI
1.4 CAMPO DI APPLICAZIONE
CAPITOLO 2: PRINCIPI GENERALI DELL'E-SAFETY
2.1 SICUREZZA E PROTEZIONE DEI MINORI
2.2 USO CONSAPEVOLE, CRITICO E RESPONSABILE DELLE TECNOLOGIE
2.3 LEGALITA' E RISPETTO DELLA NORMATIVA
2.4 RESPONSABILITA' CONDIVISA
2.5 PROTEZIONE DEI DATI E TUTELA DELLA PRIVACY
2.6 INCLUSIONE E ACCESSIBILITA'
2.7 FORMAZIONE CONTINUA
CAPITOLO 3: RUOLI E RESPONSABILITA'
3.1 DIRIGENTE SCOLASTICO
3.2 DOCENTI
3.3 STUDENTI
3.4 FAMIGLIE
3.5 PERSONALE ATA
3.6 TEAM DIGITALE/ANIMATORE DIGITALE
3.7 TEAM PER LA LEGALITA', ANTIBULLISMO E CYBERBULLISMO
3.6 REFERENTE PER IL BULLISMO E CYBERBULLISMO
CAPITOLO 4: CONDIVISIONE E COMUNICAZIONE DELLA POLICY
4.1 DESTINATARI DELLA POLICY
4.2 MODALITA' DI COMUNICAZIONE
4.3 PRESENTAZIONE E SENSIBILIZZAZIONE
4.4 OBIETTIVI DELLA COMUNICAZIONE
4.5 AGGIORNAMENTO E MIGLIORAMENTO
CAPITOLO 5: PREVENZIONE E GESTIONE DELLE INFRAZIONI
5.1 TIPOLOGIE DI INFRAZIONI
5.2. INFRAZIONI E MISURE CORRETTIVE RIVOLTE AGLI ALUNNI
5.3. INFRAZIONI E MISURE CORRETTIVE RIVOLTE AL PERSONALE SCOLASTICO
5.4. INFRAZIONI E MISURE CORRETTIVE RIVOLTE ALLE FAMIGLIE
5.5 PRINCIPI COMUNI PER TUTTE LE CATEGORIE
5.6 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA EPOLICY E SUO
5.7 AGGIORNAMENTO DELLA EPOLICY

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

DOCUMENTO DI REVISIONE/AGGIORNAMENTO
PIANO DI AZIONE PER IL TRIENNIO DI RIFERIMENTO
CAPITOLO 6: FORMAZIONE E CURRICOLO
6.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI
6.2 FORMAZIONE DEI DOCENTI SULL'USO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA
6.3 FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI
6.4 SENSIBILIZZAZIONE DELLE FAMIGLIE
CAPITOLO 7: GESTIONE DELL'INFRASTRTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA
7.1 PROTEZIONE DEI DATI PERSONALI
7.2 ACCESSO A INTERNET: FILTRI, ANTIVIRUS E SICUREZZA DELLA NAVIGAZIONE
7.3 GESTIONE DEGLI ACCESSI, PASSWORD E BACKUP
7.4 MISURE DI SICUREZZA ADOTTATE
7.5 POSTA ELETTRONICA
7.6 SITO WEB DELL'ISTITUTO COMPRENSIVO DI SAN CESARI DI LECCE
7.7 SOCIAL NETWORK
7.8 TRASPARENZA & AMMINISTRAZIONE
CAPITOLO 8: STRUMENTAZIONE PERSONALE (BYOD)
8.1 PRINCIPI GENERALI DI SICUREZZA
PIANO DI AZIONE PER IL TRIENNIO DI RIFERIMENTO
CAPITOLO 9: PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI
9.1 PREVENZIONE - RISCHI
9.2 CONTENIMENTO DEGLI INCIDENTI
9.3 RILEVAZIONE – CHE COSA SEGNALARE
9.4 GESTIONE DELLE SEGNALAZIONI
9.5 RUOLO E RESPONSABILITA' DEI DOCENTI
CAPITOLO 10: INTEGRAZIONE DELL'EPOLICY CON I REGOLAMENTI E LE POLITICHE D'ISTITUTO
ALLEGATI E LINK

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

PREMESSA

La presenza sempre più diffusa delle tecnologie digitali sta trasformando profondamente il modo in cui le nuove generazioni apprendono, comunicano e partecipano alla vita sociale. In questo contesto, la scuola ha il compito di accompagnare gli studenti nello sviluppo di competenze che permettano loro di orientarsi con autonomia e responsabilità nei nuovi ambienti interattivi virtuali.

Le competenze digitali, riconosciute dall'Unione Europea tra le otto competenze chiave per l'apprendimento permanente, *(Raccomandazione del Consiglio, 22 maggio 2018)* rappresentano oggi un presupposto fondamentale per la crescita personale e per l'inclusione culturale e professionale. La scuola, pertanto, non può considerare il digitale solo come un insieme di strumenti, ma come un ambito formativo che richiede scelte educative intenzionali e coerenti.

La Legge 92/2019, che introduce l'educazione alla cittadinanza digitale all'interno dell'Educazione Civica, determina il ruolo della scuola nella costruzione di un uso responsabile delle tecnologie. Ne deriva la necessità di una progettazione condivisa, capace di valorizzare le opportunità offerte dal digitale e di prevenire rischi e fragilità.

In questo quadro, l'Istituto Comprensivo di San Cesario di Lecce con San Donato elabora la propria **ePolicy**, un documento strategico che:

- definisce la visione educativa relativa all'uso delle tecnologie digitali e al benessere online;
- stabilisce norme comportamentali e responsabilità per studenti, personale scolastico, famiglie e soggetti esterni;
- descrive misure organizzative, tecniche e formative a tutela della sicurezza, dei dati personali, dell'inclusione e dell'accessibilità digitale;
- indica procedure per la prevenzione, la rilevazione e la gestione di comportamenti a rischio o fenomeni illeciti online (cyberbullismo, sexting, hate speech, adescamento, uso improprio dei dispositivi, violazioni della privacy, ecc.).

Riferimenti al progetto Generazioni Connesse

Il progetto è coordinato dal Ministero dell'Istruzione e del Merito, in collaborazione con Ministero dell'Interno – Polizia Postale, Autorità Garante per l'Infanzia e l'Adolescenza, Save the Children Italia, Telefono Azzurro, Università di Firenze, Università "La Sapienza" di Roma, Skuola.net, Cooperativa E.D.I. e Movimento Difesa del Cittadino.

L'Istituto Comprensivo di San Cesario aderisce alla rete Generazioni Connesse, adottando un impianto metodologico multidisciplinare e scientificamente validato per la prevenzione dei rischi digitali e la tutela dei minori online.

La presente Policy di E-Security è redatta in conformità ai materiali, ai modelli operativi e alle linee guida del Safer Internet Centre Italiano, sostenuto dalla Commissione Europea nell'ambito del programma Connecting Europe Facility – Safer Internet.

Il documento definisce principi, criteri e procedure per l'utilizzo corretto e responsabile delle tecnologie digitali da parte dell'intera comunità scolastica, nel rispetto della normativa vigente e della mission educativa dell'Istituto.

RIFERIMENTI NORMATIVI

La Policy di E-Security si colloca nel quadro delle normative vigenti in materia di cittadinanza digitale, tutela dei minori, protezione dei dati personali e sicurezza informatica, facendo riferimento a:

1. Normativa nazionale

• *Legge 13 luglio 2015, n. 107*
Riforma del sistema nazionale di istruzione e formazione.
Introduce tra le priorità formative la cittadinanza digitale e l'uso consapevole delle tecnologie.
• *Legge 29 maggio 2017, n. 71*
Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo.
Prima normativa organica per il contrasto del cyberbullismo; prevede il referente di istituto e misure educative specifiche.
• *Nota MIUR prot. 5515 del 27/10/2017*
Linee di orientamento per la prevenzione e il contrasto del cyberbullismo.
• *Legge 20 agosto 2019, n. 92*
Introduzione dell'insegnamento dell'Educazione Civica.
Include tra i nuclei tematici obbligatori la Cittadinanza Digitale.
• *Linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo – 13 gennaio 2021*
Aggiornano le linee del 2017 e rafforzano le misure di prevenzione e gestione dei casi.
• *Legge 29 aprile 2024, n. 70*
Disposizioni per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo.
Aggiorna e potenzia il quadro normativo, introducendo:

- obbligo per le scuole di adottare una Policy anti-bullismo e cyberbullismo;
- rafforzamento della rete territoriale;
- percorsi formativi obbligatori;
- misure di supporto psicologico e azioni di cittadinanza digitale.

• *DPR 8 agosto 2025, n. 134 Regolamento concernente modifiche al decreto del Presidente della Repubblica 24 giugno 1998, n. 249, recante lo statuto delle studentesse e degli studenti della scuola secondaria*, incluso l'impegno dell'istituzione scolastica e delle famiglie a collaborare per consentire l'emersione di episodi riconducibili ai fenomeni del bullismo e del cyberbullismo.
•

2. Protezione dei dati personali

• *Regolamento (UE) 2016/679 – GDPR*
Normativa europea in materia di protezione dei dati personali, particolarmente rilevante per il trattamento dei dati dei minori e per l'utilizzo di strumenti digitali e piattaforme didattiche.
• *D.Lgs. 30 giugno 2003, n. 196 – Codice della Privacy*
come modificato dal D.Lgs. 101/2018, che adegua l'ordinamento italiano al GDPR.
• *Vademecum del Garante per la protezione dei dati personali "La scuola a prova di privacy" – Edizione 2023*
Documento di riferimento aggiornato contenente indicazioni su:

- gestione di dati sensibili e particolari (es. salute, BES, DSA);
- pubblicazione di immagini e video;
- uso del registro elettronico;
- adozione di piattaforme digitali;

- comunicazioni scuola-famiglia;
- utilizzo di strumenti di intelligenza artificiale generativa.

3. Digitalizzazione e sicurezza informatica

• *Codice dell'Amministrazione Digitale – D.Lgs. 7 marzo 2005, n. 82 (CAD)*

Disciplina la digitalizzazione della Pubblica Amministrazione, con indicazioni su:

- sicurezza dei sistemi e dei dati;
- identità digitale;
- conservazione digitale;
- accessibilità e trasparenza.

• *Linee Guida AgID*

Riguardano sicurezza informatica, accessibilità, interoperabilità e standard per i servizi digitali delle istituzioni scolastiche come pubbliche amministrazioni.

• *Linee Guida MIM e AgID sull'Intelligenza Artificiale nella Scuola (2025)*

Indicano misure, responsabilità e requisiti tecnici per l'adozione di strumenti basati su IA nelle scuole, con particolare attenzione alla tutela dei dati personali e dei minori.

4. Normativa europea e programmi di riferimento

• *Programma europeo CEF – Safer Internet*

Finanzia iniziative e progetti per un Internet più sicuro, tra cui "Generazioni Connesse".

• *Linee guida eSafety* sviluppate nell'ambito dei programmi europei per la sicurezza online dei minori *(eTwinning, Better Internet for Kids).*

Stabilisce principi europei sulla tutela dei minori online, sulla sicurezza digitale e sulle competenze di cittadinanza digitale.

CAPITOLO 1: INTRODUZIONE

1.1 Scopo della Policy

La presente E-Safety Policy definisce principi, obiettivi e procedure per garantire un utilizzo sicuro, corretto e responsabile delle tecnologie digitali all'interno dell'Istituto.
In particolare, la Policy si propone di:

- **stabilire principi condivisi** da tutta la comunità scolastica sull'uso appropriato delle apparecchiature informatiche e degli ambienti digitali messi a disposizione dalla scuola;
- **salvaguardare e proteggere** bambini, ragazzi e personale scolastico da rischi legati alla navigazione online, all'uso dei dispositivi digitali e alla comunicazione in rete;
- **promuovere un uso consapevole**, critico e responsabile delle tecnologie, supportando lo sviluppo di competenze digitali, tecniche e comportamentali, nel rispetto delle norme e della cittadinanza digitale;
- **definire aspettative di comportamento chiare** per studenti e adulti, sia all'interno dell'ambiente scolastico sia durante l'uso di Internet e delle piattaforme digitali al di fuori della scuola;
- **prevedere procedure operative** per affrontare episodi di uso improprio delle tecnologie, abusi online e comportamenti lesivi, compresi i casi di bullismo e cyberbullismo;
- **garantire la consapevolezza dei rischi e delle responsabilità** legati al comportamento illecito o pericoloso, evidenziando che tali azioni sono inaccettabili e comportano adeguati provvedimenti disciplinari ed educativi;
- **monitorare percors**i, interventi e azioni collegati alla presente Policy, assicurandone l'effettiva applicazione e il miglioramento continuo.

La Scuola riconosce che gli utenti — minori e adulti — devono essere pienamente consapevoli dei rischi connessi alla navigazione in rete. Durante le attività online può accadere di imbattersi accidentalmente in contenuti inappropriati, dannosi o illegali; per questo motivo l'Istituto promuove l'adozione di strategie preventive, tra cui sistemi di filtraggio, procedure di segnalazione e un costante accompagnamento educativo.

1.2 Aree di Rischio nell'Uso delle Tecnologie Digitali

La presente Policy individua le principali ***aree di rischio*** per la comunità scolastica, distinguendole in categorie per una migliore comprensione e gestione e definisce per ognuna di queste le ***strategie di prevenzione.***

A. Rischi legati ai Contenuti (Content Risks)

Riguardano la possibilità di accedere, volontariamente o accidentalmente, a contenuti:

- inappropriati per età (violenza, linguaggio esplicito, discriminazioni);
- illeciti o pericolosi (istigazione all'odio, pedopornografia, siti non conformi alla legge);
- non attendibili o fuorvianti (fake news, truffe, disinformazione);
- che promuovono comportamenti dannosi (challenge pericolose, disturbi alimentari, autolesionismo).

Strategie di prevenzione:

- sistemi di filtraggio, educazione al pensiero critico, media literacy, segnalazione immediata al docente.

B. Rischi legati ai Contatti (Contact Risks)

Riguardano le interazioni con altri utenti online, che possono includere:

- contatti indesiderati o molesti;
- adescamento (grooming) da parte di adulti malintenzionati;

- richieste di informazioni personali o immagini private;
- manipolazioni psicologiche o ricatti emotivi.

Strategie di prevenzione:

- educazione alla comunicazione sicura, uso di piattaforme protette, non condivisione di dati personali, supporto della Polizia Postale in caso di necessità.

C. Rischi legati ai Comportamenti (Conduct Risks)

Riguardano le azioni compiute dagli stessi utenti, anche inconsapevolmente:

- comportamenti offensivi o aggressivi (cyberbullismo, hate speech);
- diffusione non autorizzata di immagini, video, dati personali propri o altrui;
- partecipazione a sfide online o pratiche dannose;
- violazioni del copyright o condivisione illegale di materiali;
- dipendenza da videogiochi o social network.

Strategie di prevenzione:

- regole chiare, responsabilizzazione degli studenti, interventi educativi e disciplinari.

D. Rischi legati alla Privacy e ai Dati Personali (Privacy & Data Risks)

Collegati alla gestione e alla protezione delle informazioni:

- violazione della privacy (trattamento scorretto di dati, pubblicazione indebita di foto);
- furto di identità digitale;
- compilazione non consapevole di moduli online o iscrizioni a servizi non idonei;
- raccolta indebita di dati da parte di app o servizi non autorizzati.

Strategie di prevenzione:

- formazione sul GDPR, uso di piattaforme conformi, autorizzazioni alle famiglie, gestione corretta degli account.

E. Rischi Tecnici e di Sicurezza Informatica (Security Risks)

Riguardano vulnerabilità dei dispositivi e delle reti:

- malware, virus, phishing, ransomware;
- accesso non autorizzato ai dispositivi o alle credenziali;
- perdita o danneggiamento accidentale dei dati;
- utilizzo improprio delle infrastrutture digitali della scuola.

Strategie di prevenzione:

- aggiornamenti regolari, password sicure, backup, uso consapevole delle reti Wi-Fi, antivirus.

F. Rischi Relativi al Benessere Digitale (Wellbeing Risks)

Riguardano l'impatto dell'uso delle tecnologie sulla salute fisica e mentale:

- sovraesposizione ai dispositivi digitali;
- riduzione delle interazioni sociali reali;
- stress, ansia, dipendenza da smartphone o social;
- disturbi posturali o visivi.

Strategie di prevenzione:

- educazione all'equilibrio digitale, pause attive, promozione di abitudini sane.

Finalità della mappatura dei rischi

La definizione di queste aree permette alla scuola di:

- attivare azioni preventive e protettive mirate;

- strutturare percorsi educativi per studenti, docenti e famiglie;
- intervenire tempestivamente in caso di episodi critici;
- garantire un ambiente digitale sicuro, inclusivo e rispettoso.

1.3 Disposizioni, Comportamenti e Procedure per l'Uso Sicuro delle Tecnologie Digitali

Il Dirigente Scolastico, i responsabili tecnici e i referenti per la sicurezza digitale, si riservano di limitare, monitorare e regolamentare l'accesso alla rete interna (Intranet) ed esterna (Internet) attraverso i normali sistemi di protezione, filtraggio e controllo previsti dagli strumenti informatici dell'Istituto.

Tali misure sono volte a prevenire comportamenti scorretti o rischiosi, tra cui:

- scaricare materiale multimediale protetto da diritto d'autore;
- visitare siti non pertinenti alla didattica o potenzialmente dannosi;
- modificare o disattivare impostazioni di sicurezza dei dispositivi;
- utilizzare la rete scolastica per fini personali o estranei all'attività educativa;
- violare norme sul copyright e sul trattamento dei dati;
- navigare su siti o servizi non consentiti dalla normativa vigente e dalla Policy di Istituto.

Disposizioni generali di sicurezza

La scuola implementa controlli periodici sui dispositivi e sulle reti, archivia i tracciati del traffico Internet secondo le normative vigenti e assicura backup regolari dei dati didattici e amministrativi. L'uso di software e dispositivi personali è consentito solo previa autorizzazione e verifica antivirus.

Eventuali anomalie o contenuti sospetti devono essere segnalati immediatamente al Dirigente, al DSGA o al referente tecnico/Animatore Digitale.

Utilizzo dei software e dei dispositivi

È vietato installare o scaricare software non autorizzati o non conformi alle licenze d'uso.

Tutte le postazioni PC in ambiente Windows sono dotate di software di protezione e blocco, che impediscono modifiche ai dati di sistema.

Le verifiche antivirus vengono effettuate regolarmente su computer, dispositivi di rete e supporti esterni.

L'utilizzo di CD, chiavette USB o dispositivi personali (BYOD) deve essere:

- autorizzato dal docente o dal personale responsabile;
- preceduto da scansione antivirus, per tutelare l'integrità della rete d'Istituto.

La scuola può limitare i siti visitabili e bloccare operazioni di download non consentite.

Gestione delle connessioni e delle credenziali

Al termine di ogni utilizzo, la connessione deve essere chiusa correttamente e l'utente deve effettuare il logout dal proprio account.

Gli utenti sono tenuti a:

- mantenere riservate e sicure le proprie password;
- non condividere credenziali con altri utenti;
- adottare password robuste secondo le linee guida nazionali (AGID – Password Policy).

In caso di smarrimento, sospetto abuso o accesso non autorizzato, l'utente è tenuto a segnalare immediatamente al referente tecnico, al DSGA o al Dirigente Scolastico.

Materiali e contenuti digitali

Il materiale didattico dei docenti può essere pubblicato sulla rete di Istituto o su siti personali solo in conformità con la presente Policy, nel rispetto:

- del copyright,

- delle licenze delle risorse digitali,
- del GDPR (in particolare per materiali contenenti foto, video o dati degli studenti).

Non è consentita la diffusione online di:

- immagini o video degli studenti senza autorizzazione;
- documenti interni riservati;
- informazioni personali sensibili.

La scuola adotta procedure di backup periodico dei dati amministrativi e didattici, al fine di garantire la continuità dei servizi e la protezione delle informazioni sensibili.

Supporto tecnico e segnalazioni

Eventuali anomalie, malfunzionamenti o contenuti sospetti devono essere immediatamente segnalati al responsabile tecnico/animatore digitale, DSGA, o al Dirigente Scolastico.

1.4 Campo di Applicazione

La presente Policy di E-Security/E-Safety si applica a tutti i membri della comunità scolastica dell'Istituto Comprensivo, senza eccezioni.

In particolare, le disposizioni contenute nel documento riguardano:

A. Studenti

- di ogni ordine e grado (infanzia, primaria e secondaria);
- durante tutte le attività didattiche, curriculari ed extracurricolari, in presenza o a distanza;
- nell'utilizzo di dispositivi, piattaforme digitali, ambienti online e strumenti informatici messi a disposizione dalla scuola.

B. Docenti

- tenuti a rispettare le norme di utilizzo delle TIC;
- responsabili della supervisione degli alunni nell'uso dei dispositivi digitali;
- incaricati di promuovere comportamenti sicuri, responsabili e legali online.

C. Personale ATA

- impegnato nella gestione tecnica e amministrativa dei sistemi informatici;
- tenuto a seguire le procedure di sicurezza per il trattamento dei dati e per l'uso dei dispositivi.

D. Dirigente Scolastico, DSGA e Responsabili di Funzione

- responsabili della governance digitale e della vigilanza sul corretto uso delle tecnologie;
- garanti dell'applicazione del presente documento e delle normative vigenti.

E. Famiglie e Tutori

- chiamati a collaborare per promuovere comportamenti sicuri anche al di fuori della scuola;
- responsabili dell'utilizzo corretto dei dispositivi personali degli studenti e del rispetto delle autorizzazioni privacy.

F. Soggetti esterni

La Policy riguarda anche:

- esperti esterni, fornitori, educatori, formatori;
- associazioni e partner coinvolti in attività didattiche o progetti digitali dell'Istituto;
- personale che acceda alle infrastrutture digitali della scuola o utilizzi piattaforme fornite dall'Istituto.

G. Ambiti di utilizzo

La Policy è applicata in tutti i contesti in cui vengono utilizzate le tecnologie digitali, quali:

- laboratori informatici, aule multimediali e spazi comuni;

- dispositivi mobili (tablet, notebook, LIM, Chromebook);
- piattaforme didattiche e amministrative (Registro elettronico Argo, Google Workspace, Microsoft 365, ecc.);
- reti interne (Intranet) e accesso a Internet;
- attività di didattica digitale integrata (DDI);
- comunicazioni istituzionali e strumenti di collaborazione online.

Finalità del Campo di applicazione

La Policy si applica a tutte le attività digitali della scuola, stabilendo regole e buone pratiche per un uso responsabile, consapevole ed etico da parte di tutta la comunità scolastica.

CAPITOLO 2: PRINCIPI GENERALI DELL'E-SAFETY

L'Istituto Comprensivo di San Cesario promuove un ambiente digitale sicuro, inclusivo e responsabile, nel quale studenti, docenti, personale scolastico e famiglie possano utilizzare le tecnologie in modo consapevole, etico e rispettoso delle normative.

La presente Policy si fonda su principi generali che guidano tutte le azioni e le decisioni relative alla sicurezza digitale**.**

2.1 Sicurezza e protezione dei minori

La sicurezza dei minori è prioritaria. La scuola adotta misure tecniche, organizzative ed educative volte a tutelare gli studenti dai principali rischi online, quali: cyberbullismo, esposizione a contenuti inappropriati, contatti indesiderati, violazioni della privacy e manipolazioni psicologiche.

Ogni intervento inerente l'e-safety ha come priorità la tutela psicologica, emotiva e fisica dei minori.

2.2 Uso consapevole, critico e responsabile delle tecnologie

L'Istituto promuove un approccio attivo e riflessivo all'uso di Internet e degli strumenti digitali, favorendo l'acquisizione di competenze che permettano agli studenti di:

- riconoscere rischi e opportunità della rete;
- utilizzare dispositivi e servizi online in maniera autonoma e rispettosa;
- comprendere le conseguenze delle proprie azioni digitali;
- adottare comportamenti etici in linea con la cittadinanza digitale.

2.3 Legalità e rispetto della normativa

L'uso delle TIC deve essere conforme alle leggi vigenti, in particolare al GDPR, al Codice Privacy, alla normativa sul diritto d'autore, alle disposizioni contro il cyberbullismo e alle regole di utilizzo dei servizi digitali scolastici. Ogni comportamento illecito, dannoso o contrario al Regolamento d'Istituto è soggetto a sanzioni proporzionate.

2.4 Responsabilità condivisa

La sicurezza digitale è un impegno comune tra:

- scuola (Dirigente, docenti, personale ATA);
- studenti;
- famiglie;
- eventuali figure esterne che collaborano con l'Istituto.

Ciascuno è chiamato ad adottare comportamenti responsabili e a segnalare tempestivamente eventuali situazioni rischiose o problematiche.

2.5 Protezione dei dati e tutela della privacy

Ogni trattamento di dati personali – in particolare immagini, video, informazioni degli alunni – avviene nel rispetto del GDPR e dei principi di minimizzazione, liceità e trasparenza. La scuola promuove un uso accurato degli account istituzionali, delle piattaforme educative e degli strumenti cloud.

2.6 Inclusione e accessibilità

L'accesso agli strumenti digitali deve essere equo e non discriminatorio.
La scuola si impegna a:

- garantire ambienti digitali accessibili anche ad alunni con Bisogni Educativi Speciali;
- utilizzare software e contenuti adeguati;
- progettare attività fruibili da tutti.

2.7 Formazione continua

L'Istituto promuove percorsi formativi periodici rivolti a:

- studenti, per potenziare consapevolezza e competenze digitali;
- docenti, per l'aggiornamento sulle pratiche sicure e sulle normative;
- famiglie, per supportare l'uso corretto delle tecnologie anche in ambito domestico.

CAPITOLO 3: RUOLI E RESPONSABILITÀ

Per garantire un ambiente digitale sicuro ed efficace, l'Istituto Comprensivo di San Cesario definisce in modo chiaro i compiti e le responsabilità delle diverse figure coinvolte nell'attuazione della E-Safety Policy. La definizione dei ruoli consente di creare una rete di responsabilità condivisa, fondamentale per la prevenzione dei rischi digitali, la tutela dei dati personali e la promozione del benessere di tutta la comunità scolastica.

3.1. DIRIGENTE SCOLASTICO

Il Dirigente Scolastico ha la responsabilità complessiva dell'attuazione della Policy e svolge un ruolo centrale nella promozione di un ambiente digitale sicuro, consapevole e conforme alla normativa vigente.
In particolare, il Dirigente:

Garantisce la sicurezza degli ambienti digitali

- Assicura la protezione dei membri della comunità scolastica, con particolare attenzione alla sicurezza online degli alunni.
- Vigila sulla corretta applicazione delle norme di sicurezza informatica e sull'uso appropriato delle tecnologie digitali all'interno dell'Istituto.
- Si avvale di sistemi e procedure di monitoraggio per individuare eventuali comportamenti rischiosi o violazioni.

Gestisce l'infrastruttura digitale e i servizi online

- Garantisce che la scuola utilizzi un Internet Service Provider (ISP) con sistemi di filtro e protezione conformi alla normativa vigente.
- Autorizza configurazioni, limitazioni o sospensioni dell'accesso a Internet in caso di rischio o utilizzo improprio.
- Supervisiona l'aggiornamento periodico dei software di sicurezza (filtri web, antivirus, firewall, backup).

Promuove formazione e cultura della sicurezza

- Assicura che tutto il personale docente e ATA riceva formazione adeguata sull'utilizzo sicuro, responsabile e inclusivo delle TIC.
- Favorisce la crescita delle competenze digitali degli alunni, anche attraverso progetti e percorsi di educazione alla cittadinanza digitale.

- Promuove interventi di prevenzione primaria per contrastare fenomeni di bullismo, cyberbullismo e uso improprio delle tecnologie.

Garantisce il rispetto delle procedure

- Si assicura che il personale scolastico conosca le procedure da attuare in caso di incidenti, violazioni della policy o segnalazioni di cyberbullismo.
- Coordina la raccolta delle segnalazioni e la gestione dei casi in collaborazione con il Referente Cyberbullismo e con il Team per la Legalità.
- Vigila sull'applicazione delle misure disciplinari in un'ottica educativa e di giustizia riparativa.

Coordina i gruppi di lavoro dedicati all'E-Safety

- Organizza e coordina il team per l'Educazione alla Legalità e al contrasto al Bullismo e Cyberbullismo.
- Favorisce la collaborazione con il Team Digitale, l'Animatore Digitale e altre figure professionali interne.

Promuove trasparenza e comunicazione

- Garantisce che il sito web della scuola includa informazioni aggiornate sulla sicurezza online, sulle procedure di segnalazione e sulle policy digitali dell'Istituto.
- Favorisce la comunicazione costante con famiglie e studenti in tema di rischi digitali, comportamenti corretti e strumenti di tutela.
- partecipa a iniziative nazionali promosse dal Ministero dell'Istruzione.

3.2 Docenti

I docenti rappresentano il principale riferimento educativo per gli studenti nell'uso delle tecnologie digitali. Essi:

Promuovono un uso sicuro e consapevole delle tecnologie

- guidano gli alunni nell'uso responsabile degli strumenti digitali e della rete;
- integrano nei percorsi didattici attività di educazione alla cittadinanza digitale, con attenzione a privacy, uso critico delle informazioni, rispetto online e sicurezza.

Vigilano e intervengono in caso di comportamenti inappropriati

- monitorano l'uso dei dispositivi durante le attività scolastiche;
- segnalano tempestivamente eventuali comportamenti a rischio, episodi di bullismo/cyberbullismo o violazioni della Policy;
- collaborano con Dirigente, Referente Cyberbullismo e famiglie nella gestione dei casi.

Utilizzano strumenti conformi alla normativa

- adottano esclusivamente piattaforme digitali autorizzate dalla scuola e conformi al GDPR;
- proteggono i dati degli alunni evitando la diffusione non autorizzata di immagini, video, informazioni personali.

Curano la propria formazione

- partecipano ai percorsi di aggiornamento proposti dall'Istituto sui temi della sicurezza digitale, del cyberbullismo e dell'uso pedagogico delle tecnologie.

3.3 Studenti

Gli studenti sono parte attiva nella costruzione di un ambiente digitale sicuro e rispettoso. Essi si impegnano a:

Utilizzare responsabilmente tecnologie e rete

- rispettare le regole stabilite dalla scuola e dal Patto di corresponsabilità;
- utilizzare dispositivi e piattaforme solo per scopi didattici e autorizzati;
- non accedere a siti inappropriati o contenuti non consentiti.

Proteggere sé stessi e gli altri

- non condividere dati personali, immagini o video senza il consenso degli interessati e della scuola;
- mantenere riservate le credenziali degli account scolastici;
- segnalare immediatamente ai docenti situazioni sospette, contenuti offensivi o episodi di cyberbullismo.

Adottare comportamenti rispettosi

- usare un linguaggio adeguato e rispettoso nelle comunicazioni digitali;
- non produrre, diffondere o partecipare a contenuti che possano danneggiare altre persone.

3.4 Famiglie

Le famiglie svolgono un ruolo essenziale nel supportare la scuola nella promozione di un uso sicuro delle tecnologie. In particolare, esse:

Collaborano con la scuola

- rispettano e fanno rispettare ai figli le regole sulla sicurezza digitale e sugli account istituzionali;
- condividono con la scuola eventuali criticità, segnali di disagio o comportamenti a rischio notati a casa.

Promuovono comportamenti sicuri anche nell'ambiente familiare

- monitorano l'utilizzo domestico di dispositivi, app e social network;
- incoraggiano un uso consapevole della rete, educando all'autoprotezione digitale.

Partecipano alla formazione

- prendono parte alle iniziative di informazione e formazione promosse dalla scuola sui temi di sicurezza online, privacy, bullismo e cyberbullismo.

3.5 Personale ATA

Il personale ATA contribuisce alla sicurezza digitale attraverso il proprio operato quotidiano. In particolare:

Gestisce e tutela le infrastrutture

- collabora nella cura e nella manutenzione delle postazioni informatiche, dei laboratori e dei dispositivi mobili della scuola;
- segnala tempestivamente eventuali malfunzionamenti o rischi legati alla sicurezza.

Rispetta le norme sulla privacy

- tratta dati personali nel rispetto del GDPR e delle linee interne dell'Istituto;
- non diffonde materiale, informazioni o documenti non autorizzati.

3.6 Team Digitale / Animatore Digitale

Il Team Digitale e l'Animatore Digitale:

Supportano l'innovazione e la sicurezza

- propongono misure tecniche per migliorare la protezione dei sistemi informatici;
- supportano i docenti nell'utilizzo delle piattaforme e degli strumenti educativi digitali.

Monitorano strumenti e procedure

- collaborano all'aggiornamento dei software di sicurezza (filtri, firewall, antivirus);
- verificano periodicamente l'efficienza delle infrastrutture e delle dotazioni tecnologiche.

Promuovono la formazione

- organizzano attività formative interne sull'uso consapevole e innovativo delle tecnologie.

3.7 Team per la Legalità, Antibullismo e Cyberbullismo

Il Team:

- coordina le iniziative educative e preventive rivolte agli studenti;
- collabora nella redazione e nell'aggiornamento dei protocolli interni;
- monitora eventuali situazioni a rischio e promuove azioni di sensibilizzazione;
- assicura un approccio educativo, riparativo e non punitivo nella gestione dei casi.
-

3.8 Referente per il Bullismo e Cyberbullismo

Il Referente:

- coordina gli interventi di prevenzione e contrasto ai fenomeni di bullismo e cyberbullismo;
- gestisce, insieme al Dirigente, le segnalazioni e gli eventuali casi;
- promuove attività formative per studenti, famiglie e personale;
- mantiene i contatti con reti territoriali, Forze dell'Ordine e servizi socio-educativi;
- partecipa alle iniziative nazionali promosse dal MIM.

Questa articolazione dei ruoli consente di creare una rete di responsabilità condivisa, essenziale per la prevenzione dei rischi digitali, la tutela dei dati e la promozione di un ambiente digitale sicuro, inclusivo e orientato al benessere di tutta la comunità scolastica.

CAPITOLO 4: CONDIVISIONE E COMUNICAZIONE DELLA POLICY

La diffusione e la comprensione della E-Safety Policy all'interno della comunità scolastica rappresentano un elemento fondamentale per garantire l'effettiva applicazione delle regole e la tutela di studenti, docenti, personale e famiglie. La scuola riconosce che la sola redazione della Policy non è sufficiente: è necessario che tutti i soggetti coinvolti siano pienamente consapevoli dei contenuti, delle procedure e dei comportamenti attesi.

4.1 Destinatari della Policy

La Policy viene condivisa con l'intera comunità scolastica e riguarda, senza eccezioni:

- tutti gli studenti dell'Istituto, di ogni ordine e grado, che devono comprendere le regole per un uso sicuro delle tecnologie e delle piattaforme digitali;
- tutti i docenti, anche coloro che svolgono attività di insegnamento per brevi periodi, che hanno la responsabilità di promuovere comportamenti sicuri e vigilare sull'uso corretto dei dispositivi;
- il Dirigente Scolastico e il Direttore dei Servizi Generali e Amministrativi, responsabili della governance digitale e della supervisione delle infrastrutture;
- tutto il personale amministrativo e i collaboratori scolastici, che operano quotidianamente a contatto con strumenti e dati digitali;
- tutti gli operatori, professionisti esterni, volontari ed educatori che interagiscono con gli studenti o partecipano a progetti digitali della scuola.

4.2 Modalità di comunicazione

La scuola adotta diverse strategie per garantire che la Policy sia accessibile, comprensibile e nota a tutti gli stakeholder:

- un'area dedicata sul sito web della scuola, dove la Policy è pubblicata in formato integrale e costantemente aggiornata;
- la bacheca del Registro elettronico, utilizzata come strumento per rendere disponibili avvisi e materiali sintetici sulla sicurezza digitale;
- invio tramite posta elettronica a tutti i membri della comunità scolastica, assicurando la ricezione e presa visione del documento.

4.3 Presentazione e sensibilizzazione

Oltre alla diffusione scritta, la Policy viene discussa e condivisa in diversi momenti e contesti:

- negli organi collegiali, come consigli di interclasse, intersezione e collegio dei docenti, favorendo la riflessione comune sulle buone pratiche e sull'uso responsabile delle tecnologie;
- durante gli incontri scuola-famiglia, dove viene promossa la collaborazione attiva tra scuola e famiglie per un uso sicuro e consapevole delle TIC e di Internet;
- nei momenti di accoglienza dei nuovi studenti e del personale, quando la Policy viene fornita insieme a tutti i documenti da sottoscrivere al momento dell'iscrizione o della stipula del contratto.

4.4 Obiettivi della comunicazione

Attraverso la condivisione e la comunicazione della Policy, l'Istituto persegue obiettivi chiari e concreti:

- garantire che ogni membro della comunità scolastica sia informato sui rischi digitali, sulle norme da rispettare e sulle procedure da seguire;
- promuovere una cultura della sicurezza digitale condivisa, in cui studenti, docenti, famiglie e personale ATA agiscano responsabilmente;
- favorire la prevenzione di comportamenti inappropriati o rischiosi, episodi di bullismo e violazioni della privacy;
- assicurare trasparenza e chiarezza nella gestione delle responsabilità, dei protocolli di intervento e delle azioni di monitoraggio.

4.5 Aggiornamento e miglioramento

La Policy non è un documento statico: la scuola si impegna a monitorarne l'efficacia e ad aggiornarla periodicamente in base a:

- evoluzioni normative e legislative;
- aggiornamenti tecnologici e cambiamenti nelle pratiche digitali;
- feedback provenienti da studenti, famiglie, docenti e personale ATA;
- casi reali e segnalazioni che richiedano l'adeguamento di procedure o strumenti di prevenzione.

In questo modo, la E-Safety Policy diventa uno strumento vivo, capace di adattarsi alle esigenze della comunità scolastica e di mantenere elevati standard di sicurezza, tutela e responsabilità digitale.

CAPITOLO 5: Prevenzione e gestione delle infrazioni

L'Istituto promuove un ambiente scolastico sereno, sicuro e inclusivo, in cui ogni forma di prepotenza, aggressione o violenza, sia reale che virtuale, è considerata inaccettabile. Per favorire relazioni positive, si incoraggia la cultura dell'ascolto e del dialogo, affinché gli studenti possano condividere le proprie difficoltà e confrontarsi in modo rispettoso e responsabile. Costruire una comunità solidale significa garantire a ciascun alunno il diritto di crescere senza violenza, ma anche il dovere di sostenere e proteggere i compagni più vulnerabili.
All'interno di questa cornice educativa, l'uso delle tecnologie digitali rappresenta un'importante risorsa didattica, ma comporta anche potenziali rischi, come l'esposizione a contenuti inappropriati o dannosi durante la navigazione in rete. Per questo motivo, la scuola integra percorsi di media literacy, attività educative mirate e procedure preventive chiare, promuovendo un approccio consapevole, sicuro e responsabile al digitale.
Nonostante tutte le misure preventive e i percorsi educativi volti a sviluppare competenze emotive, sociali e relazionali, possono comunque verificarsi episodi problematici. In questi casi, la scuola interviene rapidamente, coinvolgendo studenti, docenti e famiglie, chiarendo le regole di convivenza, applicando interventi correttivi proporzionati e attivando percorsi riparativi.
In questo modo si ristabilisce un ambiente sicuro, rispettoso e inclusivo, sostenendo la crescita complessiva, emotiva e digitale, di tutti gli studenti.

5.1 Tipologie di infrazioni

Le infrazioni possono riguardare comportamenti degli studenti, dei docenti, del personale ATA o di soggetti esterni, e sono classificate in base alla gravità e al contesto:

Infrazioni minori

- Accesso a siti non pertinenti alle attività didattiche senza finalità educativa;
- Condivisione non autorizzata di materiali digitali di bassa rilevanza;
- Utilizzo scorretto o superficiale delle piattaforme didattiche, senza conseguenze dannose.

Infrazioni gravi

- Diffusione non autorizzata di immagini, video o dati personali di studenti o personale;
- Comportamenti offensivi, aggressivi o discriminatori online, inclusi cyberbullismo e hate speech;
- Violazioni della normativa sul copyright o sull'uso di software;
- Accesso a contenuti inappropriati, dannosi o illegali;
- Tentativi di intrusione nei sistemi informatici dell'Istituto o uso improprio delle credenziali di altri utenti.

Infrazioni molto gravi

- Adescamento online (grooming), minacce, ricatti emotivi o comportamenti illegali;
- Diffusione massiva di contenuti lesivi della reputazione o della privacy di persone o gruppi;
- Comportamenti reiterati nonostante interventi educativi e comunicazioni disciplinari;
- Atti che compromettono seriamente la sicurezza dei sistemi o dei dati dell'Istituto.

La scuola adotta un approccio *educativo, preventivo e proporzionato*, orientato non solo a contrastare i comportamenti scorretti, ma soprattutto a *sviluppare consapevolezza, responsabilità e competenze di cittadinanza digitale*. Le infrazioni vengono valutate in relazione al soggetto coinvolto — studenti, personale

scolastico o famiglie — e gestite attraverso interventi adeguati alla gravità dell'atto, con l'obiettivo di favorire il recupero, prevenire la recidiva e tutelare l'intera comunità scolastica.

5.2. Infrazioni e misure correttive rivolte agli alunni

Le infrazioni commesse dagli alunni possono riguardare l'uso improprio dei dispositivi digitali, l'accesso a contenuti non idonei, la violazione della privacy, la diffusione di materiale offensivo, episodi di bullismo o cyberbullismo, danneggiamento delle attrezzature scolastiche, utilizzo delle piattaforme per finalità non consentite o comportamenti che possano esporre a rischio sé stessi o altre persone.

Ogni sospetto, rischio o violazione delle norme di sicurezza digitale deve essere segnalato tempestivamente al docente della classe e al Responsabile per la sicurezza online, che provvederà a informare il Dirigente Scolastico e il DSGA. Gli episodi che configurano situazioni di pericolo, bullismo o cyberbullismo sono gestiti nel rispetto della normativa vigente e delle procedure di tutela dei minori.

Le sanzioni rivolte agli alunni hanno sempre carattere educativo e riabilitativo e prevedono il coinvolgimento della famiglia come parte attiva del percorso formativo. Gli interventi sono proporzionati all'età dello studente, al livello di maturazione e alla gravità dell'infrazione e possono comprendere:

- ***Richiamo verbale*/ *colloquio con il dirigente scolastico*** con chiarimento immediato del comportamento scorretto.
- ***Richiamo scritto*** e annotazione sul diario/registro.
- ***Limitazione temporanea dell'uso dei dispositivi o delle piattaforme scolastiche***, garantendo comunque la continuità didattica.
- ***Convocazione dei genitori*** da parte dei docenti o del Dirigente Scolastico.
- ***Attività di riflessione guidata*** (schede, impegni scritti, colloqui individuali).
- ***Interventi di mediazione e riparazione del danno*** (scuse formali, restituzione simbolica, impegni comportamentali).
- ***Attivazione del Referente per il bullismo e il cyberbullismo***, nei casi previsti dalla L. 71/2017.
- ***Sanzioni disciplinari previste dal Regolamento di Istituto,*** per i comportamenti più gravi.
- ***Coinvolgimento dei servizi territoriali o delle autorità*** competenti, qualora il comportamento possa configurare un reato (es. sexting non consensuale, minacce, diffusione illecita di immagini, adescamento).

Parallelamente agli interventi disciplinari, la scuola promuove misure educative finalizzate alla prevenzione della recidiva e al rafforzamento delle competenze relazionali e digitali, attraverso:

- percorsi di educazione alla gestione delle emozioni e alla comunicazione responsabile;
- attività di prevenzione del conflitto e promozione dell'empatia e del rispetto reciproco nel gruppo classe;
- iniziative di cittadinanza digitale (discussioni guidate, visioni, letture, partecipazione al Safer Internet Day e ad altre campagne nazionali).

Le denunce di bullismo e cyberbullismo sono trattate secondo la L. 71/2017; i reclami relativi alla protezione dei minori seguono le procedure previste dalla normativa vigente.

L'obiettivo prioritario è garantire un ambiente scolastico sicuro, favorire comportamenti digitali consapevoli e accompagnare ogni studente in un percorso di crescita personale e civica.

5.3 Infrazioni e misure correttive rivolte al personale scolastico

Il personale docente e non docente svolge un ruolo centrale nella tutela della sicurezza digitale e nella promozione di comportamenti corretti all'interno della comunità scolastica. Per questo motivo è tenuto al rispetto delle norme previste dall'ePolicy, dal Regolamento di Istituto, dal Codice di Comportamento dei Dipendenti Pubblici (D.P.R. 62/2013), dalla normativa sulla privacy (Regolamento UE 679/2016 – GDPR) e dalle disposizioni ministeriali vigenti.
Le infrazioni da parte del personale possono riguardare, a titolo esemplificativo:

- uso improprio di dispositivi o piattaforme scolastiche;
- violazioni della privacy degli studenti, delle famiglie o dei colleghi;
- mancata vigilanza sull'uso dei dispositivi da parte degli alunni;
- diffusione o condivisione non autorizzata di immagini, documenti, password, dati sensibili;
- uso personale, non consentito o non etico delle tecnologie durante l'orario di servizio;
- comportamenti inappropriati in ambienti digitali (chat, gruppi, registri elettronici);
- mancata osservanza delle misure di sicurezza informatica definite dall'Istituto.

Ogni presunta violazione deve essere comunicata al Dirigente Scolastico, che avvia le procedure previste dalla normativa amministrativa e disciplinare. Il Dirigente può, se necessario, coinvolgere il Responsabile della Protezione dei Dati (RPD), il Responsabile per la sicurezza online, il DSGA o gli uffici competenti.

Misure correttive e sanzionatorie per il personale
Gli interventi applicati al personale si basano sui principi di proporzionalità, trasparenza e tutela della comunità scolastica. A seconda della gravità dell'infrazione possono essere adottate una o più delle seguenti misure:

- ***Richiamo verbale o colloquio formale*** con il Dirigente Scolastico.
- ***Richiamo scritto*** con invito al rispetto delle disposizioni vigenti.
- ***Formazione obbligatoria*** su sicurezza digitale, privacy o uso corretto delle tecnologie.
- ***Limitazione temporanea*** dell'accesso a specifici strumenti o piattaforme digitali, se necessario per motivi di sicurezza.
- ***Attivazione delle procedure disciplinari*** previste dal CCNL Comparto Istruzione e Ricerca, nei casi più gravi o reiterati.
- Coinvolgimento del RPD e delle autorità competenti, qualora la violazione riguardi dati personali o si configuri come reato.

Gli interventi disciplinari sono volti a ripristinare condizioni di sicurezza, a prevenire reiterazioni del comportamento e a tutelare la comunità scolastica.

5.4 Infrazioni e misure correttive rivolte alle famiglie

La collaborazione con le famiglie è elemento essenziale per garantire un ambiente digitale sicuro e responsabile. I genitori, in qualità di primi educatori, sono tenuti a rispettare le disposizioni dell'ePolicy, del Regolamento di Istituto e della normativa vigente in materia di privacy e tutela dei minori.
Le infrazioni da parte delle famiglie possono riguardare comportamenti che interferiscono con il corretto funzionamento dell'attività scolastica o che compromettono la sicurezza digitale degli studenti e del personale. Tra le situazioni più frequenti si possono includere:

- uso improprio dei canali digitali di comunicazione con la scuola (chat, gruppi, piattaforme);
- diffusione non autorizzata di foto, video o contenuti relativi alla scuola o ad altri minori;

- richiesta o condivisione di informazioni sensibili senza autorizzazione;
- pressioni indebite verso docenti o personale tramite messaggi, gruppi o social;
- accesso non autorizzato a piattaforme scolastiche con credenziali dei figli;
- mancato controllo sull'uso degli strumenti digitali da parte dei propri figli, con conseguenze su sicurezza, privacy o comportamenti a rischio;
- atteggiamenti offensivi, denigratori o aggressivi nei confronti di docenti, personale o altri studenti in contesti digitali.

Ogni violazione rilevata o segnalata viene valutata dal Dirigente Scolastico, che può attivare interventi correttivi o avviare le procedure previste dal Regolamento di Istituto e dalla normativa vigente.

Misure correttive e interventi rivolti alle famiglie
A seconda della gravità dell'infrazione, della sua eventuale reiterazione e dell'impatto sulla comunità scolastica, possono essere adottate una o più delle seguenti misure:

- ***Richiamo formale*** tramite comunicazione scritta da parte del Dirigente Scolastico.
- ***Convocazione della famiglia*** per un colloquio chiarificatore con docente, coordinatore o Dirigente.
- ***Invito alla rimozione immediata*** di contenuti digitali non autorizzati (foto, video, screenshot, messaggi diffamatori).
- ***Sospensione o limitazione dell'uso dei canali digitali*** di comunicazione con la scuola, in caso di comportamenti scorretti o offensivi.
- ***Segnalazione alle autorità competenti*** (Polizia Postale, Servizi Sociali), nei casi che configurano una violazione di legge, come diffusione illecita di immagini di minori o minacce.
- ***Coinvolgimento del RPD*** (Responsabile della Protezione dei Dati) per le infrazioni relative al trattamento dei dati personali.
- ***Partecipazione obbligatoria a incontri informativi o formativi*** dedicati a cittadinanza digitale, sicurezza online e uso consapevole delle tecnologie, quando ritenuto necessario.

Gli interventi hanno lo scopo di ristabilire condizioni di correttezza e sicurezza, promuovere la collaborazione scuola–famiglia e prevenire comportamenti futuri che possano arrecare danno agli studenti o alla comunità scolastica.
La scuola sottolinea che il corretto comportamento digitale delle famiglie è parte integrante del Patto Educativo di Corresponsabilità.

5.5 Principi comuni per tutte le categorie

Indipendentemente dal soggetto coinvolto:
Le misure adottate devono essere proporzionate, educative e orientate alla prevenzione futura.
La scuola garantisce trasparenza, riservatezza e tutela della dignità di tutte le persone implicate.
Ogni infrazione viene registrata e monitorata per individuare eventuali ricorrenze e prevedere azioni di miglioramento.

5.6 Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'Istituto Comprensivo di San Cesario garantisce un monitoraggio costante dell'applicazione della ePolicy al fine di verificarne l'efficacia, individuare eventuali criticità e assicurare un miglioramento continuo delle pratiche di sicurezza digitale e di cittadinanza responsabile. Il processo di monitoraggio coinvolge il Dirigente

Scolastico, il Referente per la Sicurezza Online, i docenti, il personale scolastico e, quando necessario, gli studenti e le famiglie.
Il monitoraggio si articola nelle seguenti azioni:

1. Osservazione sistematica delle pratiche digitali all'interno delle classi e degli ambienti scolastici, con particolare attenzione all'uso consapevole e responsabile degli strumenti e delle piattaforme digitali.
2. Raccolta e analisi delle segnalazioni relative a comportamenti inappropriati, rischi o incidenti digitali, registrando tipologia, frequenza, modalità di gestione e misure adottate.
3. Valutazione dell'efficacia degli interventi educativi e correttivi, tramite la collaborazione tra docenti, referenti e famiglie, con l'obiettivo di prevenire recidive e promuovere comportamenti adeguati.
4. Monitoraggio delle attività formative rivolte a studenti, personale scolastico e famiglie, verificandone la partecipazione, la qualità e l'impatto sul clima scolastico.
5. Verifica periodica delle misure tecniche di sicurezza, incluse configurazioni delle reti, filtri di navigazione, impostazioni delle piattaforme digitali d'Istituto e protocolli di protezione dei dati personali.
6. Rilevazione annuale dei bisogni formativi, al fine di programmare percorsi di aggiornamento e prevenzione più mirati ed efficaci.

5.7 Aggiornamento della ePolicy

La ePolicy è un documento dinamico, soggetto a revisione periodica. Il suo aggiornamento avviene:

- almeno una volta all'anno, in occasione della revisione del PTOF o della pubblicazione di nuove linee guida ministeriali e di Generazioni Connesse;
- ogni volta che emergono nuove esigenze, criticità, incidenti o cambiamenti tecnologici che rendono necessario un adeguamento delle procedure di sicurezza o degli interventi educativi;
- in seguito a modifiche legislative, normative sulla privacy o sugli obblighi di tutela dei minori online;
- a conclusione dei percorsi formativi del personale, laddove emergano indicazioni utili a migliorare procedure, ruoli o strumenti.

Il processo di revisione è affidato al Dirigente Scolastico e al Referente per la Sicurezza Online, in collaborazione con i docenti, il Team Digitale, il RPD e, quando opportuno, con una rappresentanza delle famiglie e degli studenti.
La versione aggiornata della ePolicy viene approvata dagli Organi Collegiali e resa disponibile alla comunità scolastica attraverso il sito istituzionale, i canali digitali ufficiali e gli strumenti di comunicazione interna.

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento:

ISTITUTO COMPRENSIVO DI SAN CESARIO DI LECCE CON SAN DONATO	
DOCUMENTO DI REVISIONE/AGGIORNAMENTO DELL' E-SAFETY POLICY **Integrato al PTOF e al Regolamento di Istituto**	
VERSIONE	
DATA	
AUTORE	
Approvato dal Dirigente	

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

Approvato dal Collegio Docenti			
Approvato dal Consiglio di Istituto			
Prossima data di revisione			
Modifica			
VERSIONE	**DATA**	**DESCRIZIONE**	**FIRMA** Nome del docente responsabile della sicurezza online (E-Safety Policy)

Per il monitoraggio dell'attuazione della E-Safety Policy verranno analizzati i dati raccolti annualmente, utilizzando come riferimento il documento predisposto per la valutazione interna.

ANNO	NUMERO DI SEGNALAZIONI	NUMERO DI INFRAZIONI	NUMERO SANZIONI DISCIPLINARI
ANNO SCOLASTICO ……..			

LINK DEL DOCUMENTO EDITABILE:
https://docs.google.com/document/d/1rVxOz3MdxNkysFKU2h6jJsx9cnQPQR18/edit?usp=sharing&ouid=113843217003778403970&rtpof=true&sd=true

CAPITOLO 6: FORMAZIONE E CURRICOLO

6.1 Curricolo sulle Competenze Digitali per gli Studenti

I ragazzi utilizzano quotidianamente il web, spesso con modalità più intuitive e rapide rispetto agli adulti; tuttavia, tale familiarità non garantisce competenze digitali realmente consapevoli e sicure. Come indicato dalla Raccomandazione del Consiglio Europeo sulle competenze chiave per l'apprendimento permanente, la competenza digitale implica non solo l'uso tecnico delle tecnologie, ma anche spirito critico, responsabilità e capacità di partecipazione attiva alla società digitale. Essa comprende l'alfabetizzazione informatica, la comunicazione e la collaborazione online, la creazione di contenuti digitali (compresa la programmazione), la sicurezza e la cybersicurezza, il rispetto della proprietà intellettuale, la risoluzione dei problemi e il pensiero critico.

In coerenza con tali orientamenti, l'educazione alla cittadinanza digitale deve svilupparsi lungo tre dimensioni complementari:

Tecnologica, per comprendere il funzionamento degli strumenti digitali ed evitarne un uso automatico e inconsapevole.

Cognitiva, per cercare, analizzare, utilizzare e produrre informazioni valutandone credibilità e attendibilità.

Etica e sociale, per comunicare responsabilmente, tutelare i dati personali, rispettare gli altri online e maturare consapevolezza delle implicazioni delle proprie azioni digitali.

Lo sviluppo di queste dimensioni richiede un percorso strutturato e continuativo all'interno del curricolo del primo ciclo. Per questo motivo, la competenza digitale è integrata in modo trasversale in tutte le discipline, come previsto dalle **Indicazioni Nazionali e dalle Raccomandazioni Europee**. Essa si costruisce quotidianamente attraverso attività di ricerca, produzione, collaborazione e riflessione critica mediate dal digitale.

Tutti gli insegnamenti concorrono alla formazione di un uso autonomo, responsabile e sicuro delle tecnologie. L'integrazione del digitale nella didattica è sostenuta dal **Piano Nazionale Scuola Digitale (PNSD)**, che promuove metodologie innovative, ambienti di apprendimento aggiornati e un utilizzo consapevole degli strumenti tecnologici.

In questo quadro si inseriscono anche le disposizioni del **D.M. 851/2015**, che prevedono:

- il miglioramento delle competenze digitali degli studenti;
- il potenziamento delle infrastrutture tecnologiche della scuola;
- la formazione dei docenti;
- il ruolo dell'Animatore Digitale e del Team dell'Innovazione;
- la partecipazione a progetti nazionali ed europei.

La **Legge 92/2019** sull'Educazione Civica rafforza ulteriormente la dimensione digitale, prevedendo lo sviluppo progressivo della cittadinanza digitale: valutazione critica delle fonti, comunicazione responsabile, gestione dell'identità digitale, prevenzione dei rischi online e tutela del benessere psicofisico.

Coerentemente con il Decreto Ministeriale n. 166 del 9 agosto 2025, cui sono allegate le Linee guida per l'introduzione dell'Intelligenza Artificiale nelle istituzioni scolastiche, l'Istituto Comprensivo di San Cesario di Lecce articola la competenza digitale in cinque aree:

Alfabetizzazione su informazioni e dati
(ricerca, valutazione, gestione e rielaborazione dei contenuti digitali)
Comunicazione e collaborazione

(interazione online, partecipazione alla vita civica digitale, netiquette, identità digitale)
Creazione di contenuti digitali
(produzione di materiali, copyright, licenze, programmazione di base)
Sicurezza
(protezione dei dispositivi, dei dati personali, benessere digitale, prevenzione del cyberbullismo)
Risoluzione dei problemi
(pensiero computazionale, scelta degli strumenti, creatività digitale, adattamento ai cambiamenti tecnologici)
In relazione a tali aree, la scuola promuove competenze quali:

- sviluppare strategie per ricercare, valutare e verificare informazioni, riconoscendo rischi, bias e manipolazioni;
- rispettare la netiquette e adottare comportamenti inclusivi e adeguati nei diversi ambienti digitali;
- riconoscere i rischi della comunicazione con sconosciuti online e comprendere che dietro un nickname può celarsi chiunque;
- mantenere riservati dati personali, password e informazioni sensibili;
- comprendere l'importanza del consenso digitale e non pubblicare immagini o video altrui senza permesso;
- conoscere e rispettare le norme sul diritto d'autore e sulle licenze d'uso;
- individuare le dinamiche del cyberbullismo, del sexting e del grooming, sapendo quando e a chi chiedere aiuto;
- segnalare comportamenti scorretti o pericolosi agli adulti di riferimento.

Il curricolo digitale prende forma attraverso attività laboratoriali, compiti autentici, progetti verticali e percorsi interdisciplinari che favoriscono autonomia, pensiero critico, creatività e comportamento responsabile online. La scuola monitora periodicamente l'efficacia di tali percorsi mediante rubriche valutative, osservazioni sistematiche e analisi dei bisogni, aggiornando regolarmente il curricolo in risposta all'evoluzione del contesto digitale e alle esigenze formative degli studenti.
Coerentemente con la propria missione educativa, l'Istituto promuove da sempre la ***cultura della Legalità***, attraverso percorsi finalizzati all'interiorizzazione e al rispetto delle regole, riconosciute come strumenti fondamentali per una convivenza civile, inclusiva e responsabile – anche e soprattutto negli ambienti digitali.

6.2 Formazione dei Docenti sull'Uso e l'Integrazione delle TIC nella Didattica

Nell'ambito dell'innovazione scolastica, la formazione dei docenti è elemento strategico per garantire un uso consapevole, sicuro e didatticamente efficace delle TIC. Il Piano di formazione, approvato in coerenza con la **Legge 107/2015**, integra percorsi interni ed esterni, in presenza o online, e valorizza iniziative coerenti con il PTOF.
In continuità con i corsi organizzati nell'ambito del **PNRR (D.M. 66/2023),** l'Istituto promuove percorsi di aggiornamento finalizzati a:

- sviluppare competenze digitali professionali in linea con il DigCompEdu e le Linee Guida nazionali;
- integrare le TIC nella didattica quotidiana mediante metodologie innovative (laboratori, apprendimento cooperativo, piattaforme digitali);
- rafforzare la gestione della classe digitale, sicurezza online, privacy e prevenzione dei rischi;
- favorire l'uso di risorse digitali inclusive e la progettazione interdisciplinare per la cittadinanza digitale, secondo la Legge 92/2019.

L'Animatore Digitale e il Team per l'Innovazione supportano i docenti nella progettazione di attività multimediali e nella promozione di una cultura digitale sicura, inclusiva e responsabile.

6.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
La scuola si impegna a offrire una formazione costante ai docenti sulla sicurezza online, coinvolgendoli attivamente nel programma di educazione alla E-Safety. Il percorso di formazione specifica per i docenti sull'uso consapevole e sicuro di Internet prevede sia momenti di autoaggiornamento sia sessioni di formazione individuale e collettiva, favorendo l'acquisizione di competenze pratiche e aggiornate.

6.4 Sensibilizzazione delle famiglie
La scuola promuove la partecipazione attiva delle famiglie nella tutela della sicurezza online dei propri figli, fornendo strumenti, informazioni e indicazioni pratiche per un uso consapevole delle tecnologie digitali. Attraverso incontri, webinar, materiali informativi sul sito dell'istituto e campagne di sensibilizzazione, i genitori vengono guidati a riconoscere rischi, prevenire comportamenti a rischio e sostenere l'educazione digitale dei ragazzi. L'obiettivo è creare una collaborazione costante tra scuola e famiglie, rafforzando la cultura della sicurezza e della responsabilità digitale anche fuori dall'ambiente scolastico.

CAPITOLO 7: GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.
7.1 - Protezione dei dati personali
"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino".
(cfr. http://www.garanteprivacy.it/scuola).

Ogni giorno, all'interno dell'Istituto, vengono trattati numerosi dati personali relativi agli studenti e alle loro famiglie. In alcuni casi tali informazioni possono essere particolarmente delicate, ad esempio quando riguardano aspetti sanitari, situazioni di fragilità sociale o altri dati sensibili. Un corretto trattamento dei dati personali rappresenta una condizione imprescindibile per garantire il rispetto della dignità, dell'identità e del diritto alla riservatezza di ogni persona, con particolare tutela verso i minori.
La protezione dei dati personali è riconosciuta come diritto fondamentale ***dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea ed è disciplinata dal Regolamento (UE) 2016/679 (GDPR) e dal D.Lgs. 101/2018,*** che ne ha adeguato il quadro normativo in Italia.
Anche le istituzioni scolastiche sono pertanto tenute ad assicurare la piena conformità alle disposizioni vigenti, adottando misure idonee a tutelare i dati raccolti e trattati nell'ambito delle proprie funzioni istituzionali.
In questo paragrafo dell'ePolicy vengono illustrate le principali misure adottate dalla scuola per garantire un uso corretto e responsabile delle tecnologie digitali, con particolare attenzione alla gestione dei dati personali.
L'Istituto allega, inoltre, i modelli di liberatoria conformi alla normativa vigente da utilizzare nei casi in cui sia necessario acquisire il consenso informato delle famiglie, ad esempio per riprese audio/video e per la loro

eventuale diffusione a fini didattici, informativi o divulgativi, compresa la pubblicazione su siti web istituzionali o autorizzati.
Tutto il personale scolastico è individuato quale "*incaricato del trattamento"* e opera nel rispetto dei principi del GDPR, limitando il trattamento ai dati strettamente necessari per lo svolgimento del proprio ruolo istituzionale. A ciascun incaricato vengono fornite istruzioni chiare e puntuali in merito alle procedure da seguire per garantire la protezione, la riservatezza e la sicurezza dei dati trattati.
Anche in occasione di attività di ampliamento dell'offerta formativa realizzate in collaborazione con enti esterni, la scuola assicura il rispetto delle norme vigenti e richiede preventivamente alle famiglie il consenso informato per la raccolta e l'utilizzo di immagini, video o altri dati personali degli studenti.

7.2 Accesso a Internet: filtri, antivirus e sicurezza della navigazione

L'Istituto dispone di una rete wireless protetta, il cui accesso è regolato da un controller che identifica gli utenti (docenti e studenti) tramite il dispositivo utilizzato. La rete è protetta da firewall che filtrano i contenuti inappropriati, come siti con materiale per adulti, gioco d'azzardo o incitamento all'odio.
Tutte le postazioni sono dotate di antivirus (OS o freeware) costantemente aggiornati. La scuola gestisce inoltre un dominio dedicato alla rete amministrativa (Servizi), isolato dalla rete didattica (Docenti), con backup automatico dei dati per garantire la sicurezza e l'integrità delle informazioni.
La manutenzione e l'aggiornamento dei sistemi informatici di laboratori e classi periodicamente con il supporto di un tecnico esterno.

7.3 Gestione degli accessi, password e backup

Accesso ad Internet

L'accesso a Internet costituisce oggi un diritto fondamentale della persona e una condizione essenziale per il pieno sviluppo individuale, sociale e culturale. Tale principio trova conferma nell'art. 2 della ***Dichiarazione dei diritti di Internet (Commissione per i diritti e i doveri in Internet, 2014),*** secondo cui ogni individuo ha diritto di accedere alla Rete in condizioni di parità, con tecnologie adeguate e senza discriminazioni di tipo economico, sociale o culturale.
Questo diritto è riconosciuto anche nell'ordinamento europeo: il ***Regolamento (UE) 2015/2120*** stabilisce le regole per garantire un accesso aperto e non discriminatorio a Internet (principio di open internet / net neutrality), ancora oggi pienamente vigente e oggetto di monitoraggio da parte della Commissione Europea (Rapporto di attuazione 2023).
Più recentemente, il programma europeo ***"Digital Decade Policy Programme 2030" (Decisione UE 2022/2481 e aggiornamenti 2024)*** prevede che tutte le scuole europee siano dotate di connettività ad alta velocità, infrastrutture digitali adeguate e accesso ai dispositivi necessari per rimuovere il divario digitale, in particolare per gli studenti più vulnerabili.
Parallelamente, ***il Regolamento (UE) 2022/2065 – Digital Services Act (DSA) del 2024***, introduce nuove tutele per i minori nell'ambiente digitale, imponendo alle piattaforme obblighi più rigorosi in materia di trasparenza, sicurezza e protezione dei dati.
Le **Indicazioni europee 2025** sulla tutela dei minori sottolineano inoltre l'importanza di strumenti adeguati all'età e di programmi strutturati di media literacy, rafforzando il ruolo della scuola nella formazione digitale.
Alla luce di tali riferimenti normativi, il diritto di accesso a Internet è oggi pienamente riconosciuto sia nell'ordinamento italiano che in quello europeo. La scuola, di conseguenza, rappresenta il contesto privilegiato

in cui questo diritto deve essere garantito, soprattutto per quegli studenti che non dispongono di adeguate risorse tecnologiche o connettività al domicilio.
In coerenza con tale quadro, ***il PNSD – Piano Nazionale Scuola Digitale*** conferma l'obiettivo di "***fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione, affinché il diritto a Internet diventi una realtà concreta, a partire dal contesto scolastico"***. Le tecnologie digitali, infatti, contribuiscono non solo a rendere la scuola più aperta, inclusiva e flessibile, ma permettono anche di rispondere ai cambiamenti della società contemporanea e del mondo del lavoro, promuovendo una diffusa cultura digitale, che trova il suo naturale avvio nella scuola.

Accesso a Internet nell'Istituto Comprensivo di San Cesario di Lecce

- L'accesso a Internet è disponibile in tutti i sette plessi dell'Istituto Comprensivo di San Cesario e San Donato.
- Tutte le classi della scuola primaria e secondaria sono dotate di Digital Board collegate alla rete.
- Nelle scuole dell'infanzia e nei laboratori sono presenti Digital Board mobili.
- I docenti possono utilizzare liberamente Internet per le attività didattiche.
- Gli alunni possono navigare solo in modalità guidata, usando l'account istituzionale e i dispositivi della scuola (Chromebook, laptop, tablet). Lavori collaborativi e attività online sono consentiti solo sotto supervisione e nell'ambito di progetti approvati.
- È possibile utilizzare dispositivi personali (BYOD) solo con autorizzazione del Dirigente Scolastico; credenziali e password restano personali e non trasferibili.
- Tutta la navigazione con account istituzionale è protetta da un filtro di contenuti gestito dall'Istituto, che garantisce un uso sicuro della Rete.

7.4 Misure di sicurezza adottate

Per assicurare un uso corretto e protetto della rete scolastica, l'Istituto adotta le seguenti misure:

- accesso tramite username e password personali, da mantenere riservate;
- utilizzo di password sicure e cambio immediato in caso di compromissione;
- disconnessione obbligatoria al termine delle attività e divieto di usare sessioni altrui;
- dispositivi scolastici destinati esclusivamente ad uso professionale, mantenuti in sicurezza;
- accesso remoto limitato e controllato, autorizzato solo tramite sistemi approvati;
- sistemi di backup e disaster recovery garantiti da Argo Software Spa e conservazione dei documenti ufficiali tramite Infocert S.p.A.;
- trasmissione dei dati sensibili con PEC o sistemi crittografati;
- installazione, aggiornamento e manutenzione delle infrastrutture TIC affidate a tecnici qualificati e sottoposte a verifiche periodiche.

7.5 Posta elettronica

L'account istituzionale di posta elettronica della scuola è leic853003@istruzione.it, e di posta elettronica certificata (PEC): leic853003@pec.istruzione.it
utilizzati principalmente dagli uffici amministrativi per la gestione della corrispondenza in entrata e in uscita.
Ogni docente dispone di un account personale con dominio **@docenti.comprensivosancesario.edu.it**, attivato secondo quanto previsto dall'Informativa di Google Workspace for Education e in conformità al Regolamento Europeo n. 679/2016 (GDPR) per la protezione dei dati personali di studenti e famiglie.

La posta elettronica è protetta da antivirus, mentre la posta certificata dispone anche di filtri antispam. Gli account sono destinati esclusivamente a finalità didattiche e professionali, e la scuola raccomanda di mantenere separata la posta privata da quella professionale.
In particolare, la scuola assicura che:

- gli account degli studenti siano attivati solo con autorizzazione dei genitori, con protezioni e app limitate;
- agli studenti vengano insegnate le regole di sicurezza online e la netiquette nell'uso della posta elettronica e degli ambienti e-learning;
- il personale non invii dati sensibili o soggetti a privacy tramite e-mail, se non in modalità sicura; in alternativa, si utilizzeranno comunicazioni cartacee o incontri diretti;
- in caso di ricezione di e-mail sospette o illecite da parte di alunni, docenti o personale, la scuola si metterà in contatto con gli organi di Polizia Postale.

7.6 Sito web dell'Istituto Comprensivo di San Cesario di Lecce

L'Istituto Comprensivo di San Cesario con San Donato dispone di un proprio sito istituzionale, raggiungibile all'indirizzo www.comprensivosancesario.edu.it realizzato nel rispetto delle normative vigenti in materia di accessibilità, trasparenza amministrativa e protezione dei dati personali (L. 4/2004, Linee Guida AGID 2022, GDPR 2016/679).
Sul sito dell'istituto è possibile consultare informazioni sui plessi, le circolari, la modulistica e gli avvisi.
Nella sezione Privacy è disponibile un'informativa, comprensiva di liberatoria, relativa all'uso di foto e video sui canali social dell'istituto.
La gestione del sito, l'aggiornamento dei contenuti e la verifica della loro conformità alle norme sono curati dal Dirigente Scolastico, con il supporto del DPO – Responsabile della Protezione dei Dati e del personale individuato per l'amministrazione della piattaforma.

Diritti d'autore e gestione dei contenuti

La scuola detiene i diritti sui materiali prodotti internamente e pubblicati sul sito, oppure ne utilizza altri previa autorizzazione degli aventi diritto. Tutte le risorse pubblicate sono selezionate in funzione delle finalità educative, informative e istituzionali dell'Istituto e sono sottoposte a verifica prima della pubblicazione. Non vengono inseriti banner pubblicitari o altre forme di promozione commerciale.
In caso di pubblicazione o link a materiali esterni, sono sempre indicati fonti, autori e riferimenti.

Tutela della privacy e pubblicazione di immagini

Le fotografie degli alunni, relative ad attività di classe, progettuali o uscite didattiche, sono pubblicate esclusivamente previa autorizzazione formale rilasciata dalle famiglie all'atto dell'iscrizione, nel rispetto del GDPR e del D.Lgs. 196/2003 s.m.i.
Ogni contenuto multimediale è selezionato con attenzione per garantire:

- tutela dell'identità degli studenti,
- adeguatezza e finalità educativa,
- minimizzazione dei dati personali, come previsto dal principio di privacy by default.

Servizi digitali offerti dal sito

Il sito istituzionale mette a disposizione di personale, studenti e famiglie diversi servizi integrati, tra cui:

- Registro elettronico Argo DidUp (gestito da Argo Software S.p.A.);
- Segreteria digitale Gecodoc
- Albo Pretorio online e Amministrazione Trasparente;

- Bacheca e comunicazioni alle famiglie;
- Area riservata per personale docente e ATA;
- sezioni informative dedicate ai progetti, alle attività didattiche e ai piani dell'offerta formativa.

Gli ambienti digitali esterni (Argo DidUp e Gecodoc) sono integrati nel sito tramite collegamenti sicuri; i dati restano di proprietà dell'Istituto e vengono gestiti nel rispetto delle normative sulla sicurezza informatica e sulla protezione dei dati personali.

Cookies

Il sito non acquisisce dati personali degli utenti.

L'uso dei cookies di sessione è limitato esclusivamente alla trasmissione di identificativi necessari per garantire una navigazione sicura e corretta all'interno del sito.

L'impiego di cookies permanenti è strettamente finalizzato alla raccolta di dati anonimi e aggregati, utili esclusivamente per analizzare il traffico e migliorare il livello di utilizzo e fruibilità del sito.

7.7 Social Network

L'Istituto Comprensivo di San Cesario dispone attualmente di:

- una pagina ufficiale Facebook: "Istituto Comprensivo San Cesario di Lecce con San Donato di Lecce"
- un canale Telegram per il personale docente

I social network sono gestiti dalla Dirigente Scolastica e dal personale preposto.

L'uso dei social network è finalizzato esclusivamente a attività didattiche, alla comunicazione istituzionale e a iniziative coerenti con il PNSD. Tutte le attività sono regolate dalla E-Safety Policy dell'Istituto.

Personale docente

Tutto il personale è formato e tenuto a mantenere separata la comunicazione professionale da quella privata.

Gli insegnanti e gli educatori non devono creare spazi social personali destinati agli studenti; eventuali spazi online devono essere autorizzati dalla Dirigenza e utilizzati solo per progetti didattici e documentazione dei processi di apprendimento.

La comunicazione con gli studenti deve avvenire solo tramite sistemi istituzionali e piattaforme dedicate.

Studenti e studentesse

Gli studenti sono educati a un uso sicuro e responsabile dei social network.

Vengono sensibilizzati a segnalare abusi, intimidazioni o episodi di cyberbullismo.

È vietato pubblicare nomi, immagini, video o registrazioni senza autorizzazione; la diffusione non autorizzata può comportare responsabilità legali e penali, come diffamazione o danni all'immagine.

Gli alunni sono istruiti a non esprimere giudizi sugli altri studenti o sul personale scolastico tramite i social.

Genitori

I genitori ricevono informazioni sui rischi dei social network e sulle politiche dell'Istituto, attraverso campagne di sensibilizzazione e la condivisione del presente documento.

Ulteriori materiali informativi sono disponibili nella sezione dedicata del sito web della scuola.

7.8 Trasparenza & Amministrazione

Il sito "Amministrazione trasparente" dell'istituto è disponibile online, dove vengono pubblicati piani triennali, bandi, documenti di trasparenza.

Trasparenza PA https://trasparenza-pa.net/?codcli=SC15647&node=11

Presente anche il profilo su "A Scuola di OpenCoesione" con il progetto scuola e l'indirizzo dell'istituto https://www.ascuoladiopencoesione.it/it/scuola/20154

CAPITOLO 8: STRUMENTAZIONE PERSONALE (BYOD)

L'utilizzo di dispositivi digitali personali negli ambienti scolastici richiede un quadro regolamentare chiaro, fondato su sicurezza, tutela della privacy e benessere digitale. Le disposizioni nazionali più recenti — in particolare la Circolare Ministeriale n. 5274 dell'11 luglio 2024 e la Nota MIM n. 3392 del 16 giugno 2025 — *rafforzano il divieto di utilizzo degli smartphone e degli altri dispositivi elettronici personali da parte degli studenti durante l'intero orario scolastico.*

L'Istituto Comprensivo di San Cesario di Lecce recepisce integralmente tali disposizioni, adottando un approccio equilibrato e coerente con le indicazioni del Piano Nazionale Scuola Digitale (PNSD).

In particolare:

1. Studenti

L'Istituto non consente l'uso di strumenti personali (cellulari, smartwatch, tablet, cuffie wireless, laptop privati) durante la permanenza scolastica, come previsto dalla normativa vigente.

I dispositivi devono essere tenuti spenti e riposti negli zaini per l'intera permanenza a scuola.

Uso didattico (BYOD)

La scuola può autorizzare l'uso didattico di dispositivi personali solo in casi eccezionali, nel rispetto del PNSD e delle norme sulla sicurezza digitale.

L'attivazione del BYOD è possibile esclusivamente quando:

- l'attività è progettata e richiesta formalmente dal docente;
- è stata acquisita l'autorizzazione scritta della famiglia;
- sono rispettate le misure di sicurezza, privacy e controllo da parte dell'insegnante.
- qualsiasi utilizzo al di fuori dei percorsi approvati è considerato non conforme e soggetto alle misure previste dal Regolamento d'Istituto.

2. Docenti

L'uso del cellulare durante le lezioni non è consentito. È invece ammesso l'impiego di altri dispositivi elettronici personali esclusivamente a scopo didattico e in supporto agli strumenti scolastici disponibili. Fuori dalle ore di lezione, l'uso del cellulare è consentito solo per comunicazioni personali urgenti, mentre gli altri dispositivi possono essere utilizzati per attività professionali o didattiche, integrando le risorse tecnologiche della scuola.

3. Personale ATA

È consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente, senza interferire con le proprie mansioni, mentre l'impiego di altri strumenti digitali personali è consentito esclusivamente se funzionale al lavoro e compatibile con le misure di sicurezza informatica.

8.1 Principi generali di sicurezza

In tutti i casi:

È vietato utilizzare dispositivi personali per scattare foto, registrare video o audio negli ambienti scolastici.

CAPITOLO 9: PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

L'uso delle tecnologie digitali a scuola offre grandi opportunità di apprendimento, ma comporta anche rischi legati a sicurezza, privacy e comportamenti inappropriati. Questa sezione illustra le misure adottate

dall'Istituto Comprensivo di San Cesario per prevenire, rilevare e gestire eventuali casi di uso scorretto o pericoloso delle TIC, promuovendo un ambiente educativo sicuro e responsabile per tutti gli studenti.

9.1 Prevenzione – Rischi

L'utilizzo scorretto o non autorizzato di strumenti digitali nella scuola (cellulari, tablet, PC collegati alla rete) può generare diversi rischi: diffusione di contenuti inappropriati, violazione della privacy, cyberbullismo, situazioni di disagio o pericolo per gli studenti.

Azioni di prevenzione:

- Formazione continua per docenti, studenti, famiglie e personale ATA, con attenzione all'uso consapevole delle tecnologie digitali.
- Informative per le famiglie con richiesta di liberatoria per il trattamento di dati personali (foto, video, testi) quando non strettamente necessari per funzioni istituzionali.
- Regolamentazione dell'uso dei dispositivi personali all'interno della scuola: disposizioni chiare su quando e come può essere richiesto il BYOD, abbinato a filtri web (black-list) per impedire l'accesso a siti non sicuri.

9.2 Contenimento degli incidenti

In presenza di comportamenti digitali pericolosi o scorretti:

- Se vengono diffuse immagini imbarazzanti, sessuali o offensive, la scuola promuove la loro rimozione chiedendo al provider di eliminare i contenuti.
- Si coinvolgono i genitori per eliminare dai dispositivi degli studenti i materiali offensivi, richiedendo anche ai destinatari di cancellarli. La scuola può conservare una copia per eventuali indagini interne.
- In caso di contenuti illeciti (ad es. pedopornografia), la scuola attiva immediatamente le autorità competenti (Polizia, Procura), evitando di condividere o diffondere tali contenuti.

9.3 Rilevazione – Che cosa segnalare

È fondamentale favorire un sistema di segnalazione sicuro e accessibile:

- Gli studenti possono segnalare foto o dati personali pubblicati senza consenso, commenti offensivi, minacce, contenuti sessuali inappropriati, ecc.
- I docenti, pur non potendo perquisire liberamente i dispositivi personali degli alunni, devono attivare i genitori se sospettano un uso scorretto.

9.4 Gestione delle segnalazioni

Per gestire i casi la scuola adotta un percorso chiaro e strutturato:

- Uso di strumenti ufficiali per la segnalazione adottati da Generazioni Connesse, che permettono la registrazione degli episodi.
- Utilizzo del **"Diario di Bordo"** digitale, per tracciare gli eventi e le misure adottate e creare una memoria condivisa.
- Nei casi più gravi, si attiva ***il Protocollo definito dalle Linee di Orientamento*** (Decreto Ministeriale 18/01/2021, prot. 18).
- Se la situazione giustifica un coinvolgimento esterno, si impiega il ***modulo di segnalazione alle Forze di Polizia / Autorità Giudiziaria*** previsto dalle Linee Guida.
- ***Con l'entrata in vigore del Decreto Legislativo 12 giugno 2025, n. 99, la scuola prevede l'attivazione del numero nazionale 114, per la segnalazione urgente di casi gravi o emergenziali.***

9.5 Ruolo e responsabilità dei docenti

Ogni docente ha un ruolo attivo nella prevenzione e nell'intervento:

- Deve promuovere una cultura digitale consapevole, educare gli studenti a un uso sano della rete.
- Quando emergono segnali di rischio (cyberbullismo, contenuti inappropriati, atteggiamenti preoccupanti), il docente interviene prontamente, attivando il percorso di segnalazione previsto.

La sfida educativa non è solo reagire agli incidenti, ma costruire insieme a studenti e famiglie un ambiente in cui il digitale è usato con responsabilità, rispetto e sicurezza.

CAPITOLO 10: INTEGRAZIONE DELL'EPOLICY CON I REGOLAMENTI E LE POLITICHE D'ISTITUTO

L'ePolicy si integra e completa i regolamenti e le politiche interne dell'Istituto, quali il Regolamento d'Istituto, il Regolamento per il contrasto ai fenomeni del bullismo e cyberbullismo, il Codice di Comportamento degli Studenti e delle Studentesse, il Piano Nazionale Scuola Digitale e le Linee guida per la sicurezza online.
Le disposizioni dell'ePolicy sono coerenti con le norme scolastiche già esistenti e ne rafforzano l'applicazione in materia di privacy, sicurezza digitale, uso responsabile delle tecnologie e prevenzione di cyberbullismo.
Tutti i membri della comunità scolastica (docenti, personale ATA, studenti e famiglie) devono osservare le indicazioni dell'ePolicy in sinergia con i regolamenti istituzionali, garantendo un ambiente educativo sicuro, inclusivo e rispettoso.

AZIONI

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Azioni nei prossimi tre anni

2025-2028

Ministero dell'Istruzione e del Merito
Dipartimento per l'Istruzione
Direzione Generale per gli Affari Internazionali
Uff. V

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

AZIONI

Organizzare uno o più eventi o attività volti a formare il personale dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

PIANO DI AZIONI PER L'ANNO SCOLASTICO 2025-2026

1. **Diffusione e comunicazione: condivisione della policy con studenti, docenti, personale e famiglie**
2. **Formazione e sensibilizzazione: workshop su E-Safety, cyberbullismo e uso responsabile della rete.**
3. **Monitoraggio iniziale: raccolta dati su comportamenti online e segnalazioni.**
4. **Rendicontazione: report finale su azioni svolte e criticità riscontrate.**

Via Cerundolo, 64 – San Cesario di Lecce Tel.0832/205333
C.M. LEIC853003 – C.F. 80012820751
E-mail: leic853003@istruzione.it PEC: leic853003@pec.istruzione.it
www.comprensivosancesario.edu.it

Ministero dell'Istruzione e del Merito
Dipartimento per l'Istruzione
Direzione Generale per gli Affari Internazionali
Uff. V

ISTITUTO COMPRENSIVO STATALE SAN CESARIO DI LECCE CON SAN DONATO DI LECCE

SCUOLA DELL'INFANZIA – PRIMARIA – SECONDARIA DI 1° GRADO

Piano di Azioni nei prossimi tre anni

2025-2028

1. **Formazione continua:**
Partecipazione ai seminari di Generazioni Connesse
Organizzazione di eventi di presentazione del progetto Generazioni Connesse rivolti alle studentesse e agli studenti.

2. Promozione della cultura digitale e supporto tecnico-educativo alla comunità scolastica

3. Monitoraggio e valutazione: raccolta periodica di dati e analisi dei rischi

4. Revisione della policy: Aggiornamenti annuali del documento della EPolicy in linea con normative e risultati.

Via Cerundolo, 64 – San Cesario di Lecce Tel.0832/205333
C.M. LEIC853003 – C.F. 80012820751
E-mail: leic853003@istruzione.it PEC: leic853003@pec.istruzione.it
www.comprensivosancesario.edu.it

ALLEGATI E LINK

1. Diari di bordo: https://docs.google.com/document/d/15Wdq1C9lQZsBX1WWRuNtESqjIAbw3AhF/edit?usp=sharing&ouid=117816546164194599526&rtpof=true&sd=true
2. SCHEDA DI SEGNALAZION: https://docs.google.com/document/d/1rrdFUyuIVV3O09KzoXi8NuiN5b1LkcA/edit?usp=sharing&ouid=117816546164194599526&rtpof=true&sd=true
3. LINEE DI ORIENTAMENTO per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo https://drive.google.com/file/d/1SblZ2O-gEKOrRFyK1vYjUCckDxhdZuO1/view?usp=sharing
4. Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo- aggiornamento 2021 - per le istituzioni scolastiche di ogni grado. https://drive.google.com/file/d/12d1Sgg-gEE6Hzf-VWsfZIsFG1qfRf4HE/view?usp=sharing

COMPOSIZIONE DEGLI ORGANI SCOLASTICI PERMANENTI DI PRESIDIO PER IL CONTRASTO DEL BULLISMO E DEL CYBERBULLISMO

Team Antibullismo	Colella Maria Stella – Dirigente scolastica Quarta Giuseppina – Referente scolastica *bullismo e il cyberbullismo* Pascali Stefania – Referente educazione Civica Mauro Alberto Pasquale - Responsabile per la sicurezza on line
Referente scolastico per il bullismo e il cyberbullismo	Quarta Giuseppina
Team per l'Emergenza	Colella Maria Stella – dirigente scolastica Totaro Angela – Collaboratrice dirigente Quarta Giuseppina – Referente scolastica *bullismo e il cyberbullismo* Pascali Stefania – Referente educazione Civica Caforio Faustina – Responsabile scuola secondaria 1° grado "A. Manzoni" San Cesario Zilli Loredana - Responsabile scuola secondaria 1° grado "G. Pascoli" San Donato
Tavolo permanente di monitoraggio.	Colella Maria Stella – dirigente scolastica Quarta Giuseppina – Referente scolastica *bullismo e il cyberbullismo* Pascali Stefania – Referente educazione Civica Mauro Alberto Pasquale – Animatore Digitale Battista Gianluca – Direttore dei Servizi Generali e Amministrativi Consulenti territoriali: Assistenti sociali dei comuni di San Cesario e San Donato Esperti del Consultorio familiare