ISTITUTO SCOLASTICO COMPRENSIVO
Sc. dell'Infanzia - Sc . Primaria - Sc. Secondaria di I grado
53040 CETONA (SI)
Via Martiri Della Libertà n. 4
Tel. 0578/269430 - C.F. 81004340527
Indirizzo e-mail SIIC813007@istruzione.it SIIC813007@pec.istruzione.it
Sito Internet: www.iccetona.edu.it

PROCEDURA DI GESTIONE INCIDENTI RELATIVI AI SISTEMI DI INTELLIGENZA ARTIFICIALE

1. Premessa

La presente procedura disciplina le modalità di gestione degli incidenti, anomalie, eventi critici o utilizzi impropri relativi ai sistemi di Intelligenza Artificiale (IA) utilizzati dall'Istituzione scolastica.

La procedura è finalizzata a:

- individuare tempestivamente incidenti e anomalie;
- limitare gli impatti sui diritti e le libertà degli interessati; garantire la tutela dei minori;
- assicurare adeguata supervisione umana;
- gestire gli eventuali data breach;
- garantire la conformità al GDPR e all'AI Act.

2. Ambito di applicazione

La presente procedura si applica:

- alle piattaforme di IA generativa;
- ai chatbot didattici;
- ai sistemi IA integrati nei servizi cloud scolastici;
- agli strumenti di supporto automatizzato;
- alle piattaforme IA utilizzate dal personale scolastico;
- agli strumenti IA utilizzati dagli studenti nell'ambito delle attività autorizzate.

3. Definizione di incidente IA

Per "incidente IA" si intende qualsiasi evento che:

- comprometta la sicurezza dei dati personali;
- determini utilizzo improprio della piattaforma;
- generi contenuti inappropriati;
- produca risultati discriminatori o lesivi;
- comporti perdita di controllo sui dati;
- determini accessi non autorizzati;
- provochi diffusione indebita di informazioni;
- comprometta la disponibilità o integrità dei sistemi;
- determini trattamenti non conformi al GDPR o all'AI Act.

4. Esempi di incidenti IA

Incidenti Privacy

Sono considerati Incidenti sulla privacy:

- inserimento di dati sanitari nei prompt;
- caricamento dati BES/DSA;
- condivisione non autorizzata di immagini di minori;
- utilizzo di account personali non autorizzati;
- diffusione indebita di contenuti scolastici.

Incidenti tecnologici

Sono considerati Incidenti tecnologici:

- accessi non autorizzati;
- compromissione account;
- malfunzionamenti IA;
- perdita di dati;
- errori di configurazione;
- indisponibilità della piattaforma.

Incidenti AI Act / etici

Sono considerati Incidenti AI Act / etici:

- contenuti discriminatori;
- contenuti offensivi;
- utilizzo non supervisionato dell'IA;
- utilizzo di sistemi vietati;
- profilazione impropria degli studenti;
- decisioni automatizzate inappropriate.

5. Ruoli e responsabilità

Ruolo	**Compiti**
Dirigente Scolastico	Supervisione generale
DPO/RPD	Supporto privacy e valutazione GDPR
Amministratore di sistema	Gestione tecnica incidente
Referente digitale/IA	Coordinamento operativo
Docenti	Segnalazione anomalie
Personale ATA	Collaborazione operativa

6. Obbligo di segnalazione

Tutto il personale scolastico e gli utenti autorizzati devono segnalare tempestivamente: anomalie; utilizzi impropri; violazioni dati; comportamenti non conformi; incidenti tecnici; contenuti pericolosi o discriminatori.
La segnalazione deve avvenire immediatamente al:

- Dirigente Scolastico; Referente digitale/IA;
- DPO ove coinvolti dati personali.

7. Modalità di segnalazione

La segnalazione deve contenere:

- data e ora evento;
- piattaforma coinvolta;

- soggetti coinvolti;
- descrizione incidente;
- eventuali dati personali interessati;
- eventuali screenshot o evidenze tecniche;
- misure adottate immediatamente.

8. Classificazione degli incidenti

Livello basso
Eventi senza impatto significativo: errore operativo; contenuti non corretti senza dati Personali; malfunzionamenti limitati.
Livello medio
Eventi con possibile impatto: utilizzo improprio della piattaforma; inserimento accidentale dati personali comuni; accessi non autorizzati limitati.
Livello alto
Eventi gravi: data breach; coinvolgimento dati minori; diffusione dati particolari; compromissione account multipli; utilizzo sistemi vietati; incidenti con rischio elevato per gli interessati.

9. Gestione immediata dell'incidente

In caso di incidente devono essere adottate immediatamente misure quali:

- sospensione utilizzo piattaforma;
- disconnessione account compromessi;
- modifica password;
- limitazione accessi;
- conservazione evidenze;
- blocco condivisioni;
- informazione al Dirigente Scolastico.

10. Valutazione privacy dell'incidente

Il DPO supporta l'Istituto nella valutazione:

- della natura dei dati coinvolti;
- del numero interessati;
- del rischio per i diritti e le libertà;
- dell'eventuale configurabilità di data breach;
- della necessità di notifica al Garante.

11. Gestione del data breach

Qualora l'incidente comporti violazione di dati personali, si applicano le procedure previste dagli artt. 33 e 34 GDPR.

L'Istituto valuta: necessità notifica al Garante; comunicazione agli interessati; registrazione nel Registro Data Breach; ulteriori misure mitigazione.

12. Incidenti relativi ai minori

Gli incidenti che coinvolgono dati di minori devono essere trattati con priorità elevata.

Particolare attenzione deve essere prestata a:

- immagini;
- dati scolastici;

- contenuti sensibili;
- utilizzo improprio strumenti IA;
- profilazione;
- contenuti offensivi o discriminatori.

13. Incidenti relativi all'AI Act

L'Istituto valuta eventuali incidenti connessi:

- alla trasparenza;
- alla supervisione umana;
- alla discriminazione algoritmica;
- all'utilizzo di sistemi vietati;
- alla produzione contenuti fuorvianti;
- ai rischi specifici per i minori.

14. Conservazione evidenze

Devono essere conservati: log; screenshot; comunicazioni; report tecnici; cronologia eventi; copie segnalazioni.

La documentazione deve essere conservata secondo le policy interne dell'Istituto.

15. Registro incidenti IA

L'Istituto mantiene un registro contenente:

- numero progressivo incidente;
- data;
- piattaforma coinvolta;
- descrizione;
- livello gravità;
- dati coinvolti;
- misure adottate;
- eventuale notifica Garante;
- esito finale.

16. Azioni correttive

A seguito dell'incidente possono essere adottate:

- aggiornamento policy;
- limitazione funzionalità;
- sospensione piattaforma;
- formazione aggiuntiva;
- modifica configurazioni;
- aggiornamento DPIA;
- revisione autorizzazioni.

17. Formazione e consapevolezza

L'Istituto promuove attività di:

- alfabetizzazione IA;
- formazione sicurezza;
- sensibilizzazione privacy;
- utilizzo corretto piattaforme IA;

- gestione incidenti.

18. Monitoraggio periodico

L'Istituto effettua verifiche periodiche relativamente:

- agli incidenti registrati;
- alle piattaforme utilizzate;
- alle funzionalità IA;
- alle misure sicurezza;
- alla conformità GDPR e AI Act.

19. Riesame della procedura

La presente procedura è soggetta a revisione periodica, almeno annuale; in caso di nuovi strumenti IA; in caso di modifiche normative; in caso di incidenti rilevanti.

20. Data e approvazione

Il presente documento è approvato con delibera n° 102 del 19 maggio 2026 dal Consiglio d'Istituto ed è parte integrante del PUIA dell'Istituto.

Data: 19 / 05 / 2026

Il Dirigente scolastico
Prof.ssa Filomena Valente
Il documento è firmato digitalmente
ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate
e sostituisce il documento cartaceo e la firma autografa.