Istruzioni operative per la sicurezza e la gestione delle riunioni telematiche

Premessa

Le presenti istruzioni integrano il Regolamento per lo svolgimento in modalità telematica delle riunioni degli organi collegiali e dei gruppi di lavoro e per lo svolgimento delle votazioni con strumenti elettronici e ne costituiscono parte integrante. Esse definiscono le misure di sicurezza e le buone pratiche che tutti i partecipanti e i responsabili della conduzione delle sedute sono tenuti a osservare, in coerenza con i requisiti tecnico-organizzativi dell'Allegato Tecnico MIM del 28 aprile 2026 e con la normativa in materia di protezione dei dati personali e di amministrazione digitale.

Le misure si applicano alle riunioni interamente da remoto e alle riunioni in forma mista, nonché, per la parte relativa alle operazioni di voto, alle votazioni con strumenti elettronici svolte in occasione di riunioni in presenza.

1. Piattaforme e accesso

- Le riunioni si svolgono esclusivamente sulle piattaforme autorizzate e gestite dall'Istituzione scolastica (es. *Google Workspace for Education* o Microsoft 365 *Education*), individuate dal Dirigente Scolastico quale titolare del trattamento.
- L'accesso avviene di norma tramite l'account istituzionale rilasciato dalla scuola. Ove la piattaforma lo consenta, è attivata l'autenticazione a più fattori.
- I soggetti esterni non dotati di account istituzionale (es. esperti, referenti) sono ammessi solo previo accertamento dell'identità, preferibilmente attraverso una sala d'attesa virtuale gestita dall'organizzatore.
- Il link di accesso è personale e riferito alla singola seduta: non deve essere diffuso, pubblicato o condiviso con persone non autorizzate.
- È vietato l'uso di credenziali condivise o impersonali: ciascun accesso deve essere riconducibile in modo univoco a un soggetto avente diritto.

2. Dispositivi e postazione di lavoro

- Utilizzare dispositivi aggiornati, con sistema operativo e browser aggiornati e con protezione antivirus attiva.
- Collegarsi tramite connessioni protette; evitare reti Wi-Fi pubbliche e non protette. Ove necessario, utilizzare gli strumenti di connessione sicura messi a disposizione dalla scuola.
- Collegarsi da un luogo appropriato e riservato, evitando la presenza di persone non autorizzate e la possibilità che terzi ascoltino o visualizzino i contenuti della riunione.
- Non lasciare la postazione incustodita durante la seduta; bloccare lo schermo in caso di allontanamento temporaneo.
- Mantenere la webcam accesa per l'identificazione e la partecipazione attiva; disattivare il microfono quando non si interviene.

3. Gestione delle credenziali

- Le credenziali di accesso sono personali e non cedibili; non devono essere comunicate a terzi né annotate in luoghi accessibili.

- Non memorizzare le password su dispositivi condivisi o pubblici.
- In caso di smarrimento, sospetto utilizzo indebito o compromissione delle credenziali, darne immediata comunicazione al Dirigente Scolastico o al referente per la sicurezza informatica per la loro tempestiva sostituzione.

4. Ruoli e conduzione della seduta

Chi presiede la seduta e chi svolge le funzioni di organizzatore e segretario adottano le seguenti cautele:

- controllare gli ingressi tramite la sala d'attesa, ammettendo i soli aventi diritto e rimuovendo eventuali partecipanti non autorizzati;
- assegnare a ciascun partecipante il solo ruolo necessario (es. relatore, componente), secondo il principio del minimo privilegio;
- verificare l'identità dei partecipanti e la sussistenza del numero legale prima dell'avvio dei lavori;
- monitorare i partecipanti collegati durante la seduta e chiudere correttamente la sessione al termine dei lavori;
- dichiarare all'inizio della riunione eventuali registrazioni, secondo quanto previsto dal Regolamento.

5. Riservatezza e condivisione dei documenti

- La documentazione della riunione è condivisa esclusivamente con i componenti legittimati, attraverso i canali istituzionali; è vietato l'inoltro o la diffusione a soggetti non autorizzati.
- In caso di condivisione dello schermo, mostrare unicamente i contenuti pertinenti, chiudendo preventivamente finestre, applicazioni e notifiche estranee alla riunione.
- I partecipanti garantiscono la riservatezza di quanto trattato nella seduta, con particolare attenzione ai dati personali dei soggetti coinvolti.

6. Registrazioni

- La registrazione della riunione costituisce misura eccezionale e può essere disposta esclusivamente dall'Istituzione scolastica, per le finalità istituzionali indicate dal Regolamento, ed è dichiarata all'inizio della seduta.
- È vietata qualsiasi registrazione audio o video da parte dei singoli partecipanti o di terzi senza preventiva autorizzazione dell'Istituzione scolastica e senza il consenso scritto di tutti i presenti.
- Le registrazioni autorizzate sono conservate per il tempo strettamente necessario (di norma non superiore a 30 giorni) e non possono essere diffuse o utilizzate per scopi diversi da quelli istituzionali.

7. Sicurezza delle operazioni di voto

Le votazioni con strumenti elettronici, sia da remoto sia in presenza, si svolgono nel rispetto degli articoli 11, 12 e 13 del Regolamento. In particolare:

- utilizzare esclusivamente strumenti la cui conformità ai requisiti sia stata verificata preventivamente dalla scuola;

- per il **voto palese**: accesso con account istituzionale, limitazione a una sola risposta per avente diritto, raccolta dell'identità del votante e disattivazione della modifica della risposta dopo l'invio; esportazione e conservazione dei risultati a corredo del verbale;
- per il **voto a scrutinio segreto**: utilizzare unicamente un sistema di voto conforme ai requisiti dell'art. 11.3 del Regolamento; gli strumenti di raccolta moduli o sondaggio di uso corrente (es. Google Moduli, Microsoft Forms) non sono idonei allo scrutinio segreto, né a distanza né in presenza. In mancanza di un sistema conforme, la votazione segreta si svolge con scheda cartacea;
- conservare le evidenze delle operazioni di voto e allegarle al verbale secondo gli articoli 14 e 15 del Regolamento;
- in caso di malfunzionamento che comprometta l'integrità, l'univocità o la segretezza del voto, sospendere la votazione e, se necessario, ripeterla, dandone atto nel verbale.

8. Gestione degli incidenti di sicurezza

- Qualsiasi evento anomalo — accesso non autorizzato, compromissione di credenziali, intrusione, indebita divulgazione di dati personali, malfunzionamento rilevante — deve essere segnalato senza ritardo al Dirigente Scolastico e, ove individuati, al referente per la sicurezza informatica e al Responsabile della protezione dei dati (DPO).
- Il segnalante non tenta di risolvere autonomamente l'incidente e, per quanto possibile, preserva ogni elemento utile alla ricostruzione dell'accaduto.
- Qualora l'evento configuri una violazione di dati personali (data breach), il Dirigente Scolastico, quale titolare del trattamento, valuta gli adempimenti previsti dagli articoli 33 e 34 del Regolamento (UE) 2016/679, inclusa l'eventuale notifica al Garante entro 72 ore e la comunicazione agli interessati.

9. Misure tecniche a carico dell'Istituzione scolastica

L'Istituzione scolastica, con il supporto del fornitore o partner tecnologico, assicura in relazione alle piattaforme e agli strumenti adottati:

- la cifratura dei dati e l'utilizzo di connessioni protette (https/TLS);
- la protezione da vulnerabilità note e l'aggiornamento periodico dei sistemi;
- il monitoraggio e la registrazione degli accessi e la disponibilità di sistemi di audit;
- la segregazione degli ambienti e la corretta gestione delle sessioni (tracciamento delle sessioni attive, interruzione automatica in caso di inattività, prevenzione di accessi simultanei non autorizzati);
- le misure di continuità operativa, inclusi sistemi di backup e procedure di ripristino;
- per i servizi cloud o di terze parti: la verifica della localizzazione dei dati, delle misure di sicurezza dichiarate dal fornitore e della conformità alle normative europee e nazionali, nonché la nomina del fornitore a responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679.

10. Riferimenti

- Regolamento per lo svolgimento in modalità telematica delle riunioni degli organi collegiali e dei gruppi di lavoro e per lo svolgimento delle votazioni con strumenti elettronici;

- Nota MIM prot. n. 3803 del 30 giugno 2026 e Allegato Tecnico del 28 aprile 2026;
- Regolamento (UE) 2016/679 (GDPR) e D.lgs. 196/2003;
- D.lgs. 82/2005 (Codice dell'Amministrazione Digitale) e Linee guida AgID in materia di sicurezza ICT, identità digitale e conservazione dei documenti informatici;
- Provvedimento del Garante per la protezione dei dati personali 9 dicembre 2021, n. 215.

Il Dirigente Scolastico