ISTITUTO COMPRENSIVO ROTONDA VIGGIANELLO di Rotonda (PZ)
Prot. 0007753 del 12/11/2025
I-4 (Uscita)

Linee guida specifiche per il personale amministrativo

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

1. Garantire la segretezza delle credenziali riservate per l'accesso a qualunque area riservata connessa al proprio incarico. Si rammenta, inoltre, che non è consentito memorizzare tali credenziali nei browser.
2. Acquisire i certificati medici esibiti dagli alunni a giustificazione delle assenze (o qualunque altro documento contenente dati personali o particolari) direttamente dei collaboratori scolastici delegati alla consegna in segreteria.
3. Le copie della documentazione relativa ai Piani Didattici Personalizzati e i Piani Educativi Individuali sottoscritti dai docenti e dai genitori devono essere autorizzate dal titolare del trattamento e saranno prive dei dati personali che possano consentire l'individuazione dell'alunno.

Nell'uso dei PC e delle dotazioni tecnologiche dell'Istituto è necessario attenersi alle seguenti istruzioni operative:

1. È vietato l'utilizzo di Pen Drive, Hard Disk portatili e ogni altro dispositivo di storage personale, ovvero l'utilizzo di tali dispositivi è condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;
2. È vietato memorizzare documenti sui PC della scuola;
3. Curare la conservazione e la segretezza delle proprie credenziali di accesso alle diverse aree riservate; Le password impostate devono essere di tipologia "forte", intendendosi una combinazione casuale di lettere (maiuscole e minuscole), numeri, caratteri speciali, in alcun modo riconducibile al titolare dell'account.
4. È vietata la consultazione della propria casella di posta elettronica sui PC della scuola;
5. Nel caso in cui sia necessario accedere ad un proprio account di servizi cloud (ad esempio Google Drive), al termine dell'utilizzo assicurarsi che sia avvenuta la disconnessione dal proprio account.
6. Comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
7. Spegnere correttamente il computer al termine di ogni sessione di lavoro, evitando di abbandonare la propria postazione di lavoro senza averla spenta.

Linee guida specifiche per il personale ausiliario

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

Nell'uso dei PC e delle dotazioni tecnologiche dell'Istituto è necessario attenersi alle seguenti istruzioni operative:

1. Garantire la segretezza delle credenziali riservate per l'accesso a qualunque area riservata connessa al proprio incarico. Si rammenta, inoltre, che non è consentito memorizzare tali credenziali nei browser.
2. È vietato l'utilizzo di Pen Drive, Hard Disk portatili e ogni altro dispositivo di storage personale, ovvero l'utilizzo di tali dispositivi è condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;
3. È vietato memorizzare documenti sui PC della scuola;
4. Curare la conservazione e la segretezza delle proprie credenziali di accesso alle diverse aree riservate; Le password impostate devono essere di tipologia "forte", intendendosi una combinazione

casuale di lettere (maiuscole e minuscole), numeri, caratteri speciali, in alcun modo riconducibile al titolare dell'account.
5. È vietata la consultazione della propria casella di posta elettronica sui PC della scuola;
6. Nel caso in cui sia necessario accedere ad un proprio account di servizi cloud (ad esempio Google Drive), al termine dell'utilizzo assicurarsi che sia avvenuta la disconnessione dal proprio account.
7. Comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
8. Spegnere correttamente il computer al termine di ogni sessione di lavoro, evitando di abbandonare la propria postazione di lavoro senza averla spenta.

Linee guida specifiche per il personale docente

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

1. Garantire la segretezza delle credenziali riservate per l'accesso al registro elettronico o a qualunque area riservata connesse al proprio incarico. Si rammenta, inoltre, che non è consentito memorizzare tali credenziali nei browser.

2. Consegnare i certificati medici esibiti dagli alunni a giustificazione delle assenze (o qualunque altro documento contenente dati personali o particolari) tempestivamente al collaboratore scolastico, avendo cura che nessuno possa prenderne visione. Il collaboratore scolastico avrà l'obbligo della trasmissione immediata in segreteria.

3. Per i plessi o le sezioni distaccate prive di ufficio di segreteria, la documentazione riservata di cui al punto precedente, dovrà essere consegnata al collaboratore scolastico preposto, che avrà l'obbligo di consegnarli tempestivamente in segreteria.

4. I Piani Didattici Personalizzati e i Piani Educativi Individuali sottoscritti dai docenti e dai genitori, devono essere tempestivamente consegnati in segreteria. Eventuali copie di tali documentazioni devono essere autorizzate dal titolare del trattamento e saranno prive dei dati personali che possano consentire l'individuazione dell'alunno.

5. È vietata, nell'alveo delle funzioni istituzionali, la condivisione e la comunicazione/diffusione di messaggi, foto e immagini riguardanti gli alunni attraverso le APP di messaggistica online (ad es. Whatsapp, Telegram) e sui profili social network personali (ad es. Facebook, Twitter, Instagram). Eventuali comportamenti in difformità di quanto definito sono attivati sotto la piena responsabilità civile e penale del singolo docente.

Nell'uso dei PC e delle dotazioni tecnologiche dell'Istituto è necessario attenersi alle seguenti istruzioni operative:

1. È vietato l'utilizzo di Pen Drive, Hard Disk portatili e ogni altro dispositivo di storage personale, ovvero l'utilizzo di tali dispositivi è condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;

2. È vietato memorizzare documenti sui PC della scuola;

3. Curare la conservazione e la segretezza delle proprie credenziali di accesso al registro elettronico e ad ogni altra area riservata; Le password impostate devono essere di tipologia “forte”, intendendosi una combinazione casuale di lettere (maiuscole e minuscole), numeri, caratteri speciali, in alcun modo riconducibile al titolare dell’account.

4. È vietata la consultazione della propria casella di posta elettronica sui PC della scuola;

5. Nel caso in cui sia necessario accedere ad un proprio account di servizi cloud (ad esempio Google Drive), al termine dell’utilizzo assicurarsi che sia avvenuta la disconnessione dal proprio account.

6. Comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;

7. Spegnere correttamente il computer al termine di ogni sessione di lavoro, evitando di abbandonare la propria postazione di lavoro senza averla spenta.