Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

AUDIT DI VALUTAZIONE CONFORMITA' AL GDPR 679/2016 PER LA GESTIONE DATI PERSONALI

TITOLARE DEL TRATTAMENTO
Istituto professionale Alberghiero Di Spoleto

RESPONSABILE DELLA PROTEZIONE DEI DATI
Oxfirm srl Viale Antonio Ciamarra 259 – 00173, ROMA (RM) Tel: 06-86356274; e-mail: **privacy@oxfirm.it** nella persona di: **Ing. Antonio Bove, tel.: 3397775992**

INFORMAZIONI GENERALI	
Numero di plessi:	2
Numero di plessi coperti da rete:	2
Numero di postazioni amministrative (incluso DS e DSGA):	11
Dirigente Scolastico	Roberta Galassi
DSGA	-

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

AUDIT DI VALUTAZIONE CONFORMITA' AL GDPR 679/2016 PER LA GESTIONE DATI PERSONALI

INCARICATI	
Animatore digitale o Team:	Prof. Paola Selli
Collaboratori del DS	Prof. Paola Selli, prof.ssa Antonella Bonifanzi, incaricato formalmente
Responsabile sito web interno:	Paolo Ciri, incaricato formalmente
Responsabile pubblicazione sito web:	Paolo Ciri, incaricato formalmente
Responsabile pubblicazione piattaforme social:	Paolo Ciri, Roberta Bizzaglia, incaricato formalmente
Responsabile piattaforma DDI	Paolo Ciri,
Responsabile rilascio password piattaforma DDI	,
Assistente Tecnico interno:	Fabio Gentili, incaricato formalmente
Amministratore di sistema interno:	-, non presente
Utilizzo piattaforma Google for education o Microsoft	
Responsabile di plesso:	Paola Selli, Antonella Bonifanzi, succursale: Katia polito, Fabio Mamone, succursale sede coordinata: Emanuele Pilati, Roberta Testacuzza, sede casa di reclusione: Maria Pascale, incaricato formalmente
Referente Privacy:	-, incaricato formalmente

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

RESPONSABILI ESTERNI DEL TRATTAMENTO	
Gestionale Segreteria:	Gruppo Spaggiari Parma S.p.A.
Registro Elettronico:	Gruppo Spaggiari Parma S.p.A.
Fornitore assistenza tecnica:	-, Non presente
RSPP:	Fabio Moscione, Roberto Quadraccia, incarico formalizzato
Medico competente:	Fioriti Cristina, incarico formalizzato
Psicologo:	-, Non presente

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

PRINCIPI DI VALUTAZIONE E STRUTTURA DELL'ANALISI: MISURE DI SICUREZZA

A seguito della verifica effettuata dal Responsabile della Protezione dei dati, in data 10/01/2025 è stato rilevato lo stato delle Misure di Sicurezza.

MISURE DI SICUREZZA TECNICHE FISICHE

Per approntare delle **misure di sicurezza "adeguate"** è necessario valutare una serie di fattori quali:

a. **le modalità di accesso ai locali**, definendo le aree e gli orari in cui potrà essere consentito l'accesso al pubblico o al personale non autorizzato
b. **la qualità delle protezioni esterne**: porte e serrature; presenza di allarmi, illuminazione di sicurezza o CCTV (telecamere)
c. la corretta gestione e **smaltimento dei rifiuti** cartacei o elettronici
d. **l'impostazione delle apparecchiature informatiche** e le politiche del loro utilizzo, incluse quelle di proprietà dell'utente quando queste possono connettersi alla rete della amministrazione.
e. Inoltre, tra le indicazioni di AgID, vi è quella della tenuta di **un registro con l'indicazione delle risorse informatiche utilizzate** per trattare dati, la loro ubicazione fisica e i permessi di accesso alle stesse, ecc.).

Nel corso della verifica è stato rilevato lo stato delle seguenti misure di sicurezza tecniche e fisiche:

1. L'ingresso all'edificio è presidiato da collaboratori scolastici, l'accesso all'edificio avviene previo utilizzo di campanello.
2. L'accesso agli uffici amministrativi è presidiato da collaboratori scolastici, l'accesso agli uffici amministrativi avviene previo utilizzo di campanello.

3. Gli uffici amministrativi sono tutti collocati in una sezione dedicata dell'edificio.
4. Negli uffici amministrativi sono presenti: chiusura a chiave, armadi con serratura, casseforti/armadi blindati.
5. Presenza di un front office: è presente un front office per gli alunni e famiglie, è presente un front office per il personale

   (Il front office consente di organizzare l'accoglienza di genitori, studenti ed insegnanti, limitare l'accesso di personale estraneo all'interno degli uffici amministrativi e di tutelare la privacy e la sicurezza dei dati.)
6. Il sistema di videosorveglianza: copre l'area perimetrale.
7. La gestione della videosorveglianza è interna.
8. La conservazione dei dati (luogo) è interna.
9. Accesso a NAS/NVR/DVR con password: presente.
10. Dispositivo di conservazione in armadio protetto: presente.
11. Sistema di conservazione criptato: presente.
12. Monitor ripresa in diretta: non è presente.
13. Regolamento Videosorveglianza: Non approvato.
14. Accordo RSU: Non stipulato.
15. Autorizzazioni al trattamento di videosorveglianza: No.
16. Gruppi di continuità: sono presenti in parte delle postazioni amministrative, presente solo sul/sui server.
17. È presente un sistema di distruzione dei documenti cartacei.

    (È importante garantire la sicurezza dei dati attraverso la distruzione di documenti o fotocopie non più utilizzati. È consigliabile custodire i documenti cartacei e i supporti informatici removibili in scaffali chiusi a chiave e al termine dell'orario di lavoro riporre tutti i documenti presenti sulla scrivania in cassetti chiusi a chiave.)

Misure di sicurezza suggerite:

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

MISURE DI SICUREZZA TECNICHE LOGICHE

Nel corso della verifica è stato rilevato lo stato delle seguenti misure di sicurezza logiche:

A. Misure digitali

1. Dominio Windows: non è presente.
2. Sistema di back-up in rete locale: è presente.
3. Sistema di back-up in cloud: è presente.
4. Accesso a cartelle condivise (con password) su Server/NAS: è presente.
5. Firewall: è presente.
6. Gestione di presenze elettronica: è presente.
7. Gestione di presenze cartacea: non è presente.
8. Separazione fisica o logica delle reti LAN per la didattica e la segreteria: è presente.
9. Sistema di stampanti di rete: è presente.

B. Configurazione PC

- Per la **segreteria** sono presenti le seguenti misure di sicurezza per il PC:

aggiornamenti automatici sistemi operativi, aggiornamenti antivirus automatizzati, accesso tramite password.

- Per la **didattica** sono presenti le seguenti misure di sicurezza per il PC:

aggiornamenti automatici sistemi operativi, aggiornamenti antivirus automatizzati.

Ricordiamo che è consigliabile che le misure di sicurezza per i PC prevedano sempre:

1. creazione di **doppio account** (amministratore e utente limitato) protetti da password
2. impostazione degli **aggiornamenti** del sistema operativo, dell'antivirus e di tutte le applicazioni automatiche

3. sospensione automatica delle sessioni di lavoro (screensaver con password), con un tempo di attivazione non superiore ai 5 minuti e con riavvio protetto da password
4. **password di accesso** di complessità adeguata (contenenti almeno 8 caratteri, maiuscole, minuscole, lettere e numeri ed un carattere speciale), da cambiare periodicamente.
   Si consiglia di non annotare le password create e/o modificate su foglietti custoditi nei pressi della postazione o sotto la tastiera, ma di consegnarle in busta chiusa all'amministratore di sistema. Si consiglia, infine, di custodirle in armadi chiusi a chiave.
   Ogni cambio di password dovrà essere appositamente annotato nel relativo registro
5. **accessi logici** e di autenticazione ad applicativi e cartelle condivise secondo ruoli e responsabilità definiti
6. **profili personali** attribuiti agli utenti al fine di migliorare la sicurezza e la gestione dei dati archiviati
7. trattamento separato, in partizioni diverse, dei dati particolari e/o giudiziari rispetto ai dati non particolari e/o giudiziari, con appositi controlli di sicurezza
8. registrazione di ogni intervento e/o modifica eseguita nel sistema informatico da parte dell'amministratore, con annotazione della data/orario dell'ultima modifica
9. verifica periodica delle attrezzature informatiche
10. verifica periodica dell'operato degli addetti alla manutenzione.

In ogni caso sarebbe opportuno conformarsi alle indicazioni di AgID in materia di misure minime di sicurezza per le pubbliche amministrazioni (circolare AgID 2/2017).

C. Navigazione internet

- Per la **segreteria** sono presenti le seguenti misure di sicurezza per la navigazione internet:

autenticazione univoca alla rete Wi-Fi con account e pw personali, filtraggio della navigazione, aggiornamento black list internazionali.

- Per la **didattica** sono presenti le seguenti misure di sicurezza per la navigazione internet:

filtraggio della navigazione, aggiornamento black list internazionali.

Ricordiamo che è consigliabile che le misure di sicurezza per la navigazione internet

includano sempre:

1. autenticazione univoca alla rete Wi-Fi (account e password personali)
2. accesso da remoto tramite VPN
3. filtraggio della navigazione
4. aggiornamento black list internazionali
5. blocco traffico da geolocalizzazione

E' consigliabile, inoltre, effettuare gli aggiornamenti delle black list il più frequentemente possibile e, comunque, ad intervalli non superiori ad una settimana.

Bisogna implementare un sistema di captive portal per gestire gli account Wi-Fi

---

D. Gestione dati

Si consiglia di:

1. definire le **procedure** per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: presente.
2. verificare periodicamente lo **stato delle attrezzature**, tramite l'amministratore di sistema: non presente.
3. verificare l'operato degli addetti alla manutenzione: non presente.

MISURE DI SICUREZZA ORGANIZZATIVE

L'art. 5, par. 1, lett. f) del **GDPR** dispone il trattamento dei dati personali "*in maniera da garantire un'**adeguata sicurezza**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*".

La *sicurezza* a cui si riferisce la normativa riguarda l'intero aspetto organizzativo posto alla base dei processi di trattamento:

a. registro del Titolare, informativa per il trattamento dei dati personali dei fornitori, informativa per il trattamento dei dati personali dei dipendenti, informativa per il trattamento dei dati personali degli alunni e delle famiglie, incarico collaboratori scolastici

e personale ausiliario, organigramma Privacy

Ricordiamo che il **Registro del Titolare del Trattamento** rappresenta uno strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità. Esso è altresì uno strumento fondamentale e indispensabile per ogni valutazione e analisi del rischio. Si ricorda che tale registro, oltre ad essere datato e protocollato, andrà necessariamente aggiornato e modificato ogni volta in cui i trattamenti ivi indicati subiranno delle modifiche.

Si consiglia inoltre:

1. la predisposizione e pubblicazione sul sito web della scuola, nella sezione privacy, delle **informative** riguardanti il trattamento dei dati dei fornitori, dipendenti e alunni delle famiglie. Il Titolare del trattamento, la Scuola, in virtù del principio dell'*accountability*, dovrà dare massima diffusione alle stesse su vari canali (es.: pubblicazione sul sito istituzionale della scuola in un'apposita sezione PRIVACY posta in calce alla pagina e sempre visibile, posta elettronica, registro elettronico, ecc...)
2. la designazione dei **Responsabili esterni del trattamento** dei dati. A tal proposito si precisa che dovranno essere nominati responsabili esterni del trattamento dei dati le persone, fisiche o giuridiche, legate all'Amministrazione da un contratto avente natura continuativa, non occasionale, trattanti i dati personali per conto del Titolare del Trattamento, la Scuola (es.: il gestore del registro elettronico e contabilità, l'amministratore di sistema esterno).
   Potranno essere, inoltre, nominati responsabili esterni del trattamento dei dati: il medico del lavoro, il responsabile della sicurezza, gli esperti esterni.
   In assenza di tale nomina sarebbe comunque opportuno integrare i relativi contratti con clausole di riservatezza previste nel modello di responsabile esterno del trattamento
3. l'individuazione di un **amministratore di sistema** interno o esterno all'Istituzione Scolastica che avrà il compito di sovrintendere all'aggiornamento dei sistemi operativi, delle applicazioni e di tutte le attrezzature secondo le indicazioni fornite dal Titolare del trattamento
4. le designazioni del **personale incaricato**/autorizzato al trattamento dei dati personali, sottoscritti dal personale interessato per presa visione
5. la compilazione del **diario della privacy** all'interno del quale annotare le attività eseguite per la conformità dell'Istituzione Scolastica al reg. UE 2016/679 nonché tutti gli incontri, colloqui telefonici, mail intercorse con il Responsabile della Protezione dei Dati.

Oxfirm s.r.l.
Sede legale: Viale Antonio Ciamarra 259 – 00173, ROMA (RM)
Partita IVA: 15972861007
Tel. 06.86356274
email: privacy@oxfirm.it
www.oxfirm.it

Roma, 10/01/2025

Ing. Antonio Bove