Ministero dell'Istruzione, dell'Università e della Ricerca - Ufficio Scolastico Regionale per il Lazio

ISTITUTO TECNICO AGRARIO "GIUSEPPE GARIBALDI"

REGIONE LAZIO

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005

Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007

E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Prot. n 7240/1.5.b Roma, 20/06/2018

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ai sensi del REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
(Testo rilevante ai fini del SEE)

misure di sicurezza nel trattamento dei dati personali e piano operativo per l'adozione delle misure minime di sicurezza - 2018

Il Dirigente Scolastico

Visto il REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) Codice in materia di protezione di dati personali, Disciplinare tecnico in materia di misure minime di sicurezza.

Considerato che l'Istituzione Scolastica "Istituto Tecnico Agrario "Giuseppe Garibaldi", con sede in Via Ardeatina 524, Roma in quanto dotata di un autonomo potere decisionale, ai sensi dell'art.28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

Atteso che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza, adotta il presente

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

Finalità:

Al fine di perseguire le finalità istituzionali, l'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori. I trattamenti sono effettuati, anche mediante strumenti elettronici e informatici, per le seguenti finalità:

- adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- somministrazione dei servizi formativi;
- gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);
- adempimenti assicurativi;
- tenuta della contabilità;
- gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n.150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";
- attività strumentali alle precedenti.
- tenuta del **registro dei trattamenti** prevista dall'articolo 30 del Regolamento Generale Europeo, l'onere della tenuta del registro è a carico del titolare e, se nominato, del responsabile del trattamento.

Registro dei trattamenti**: c**ontenuto minimo.

Il registro deve elencare una serie di informazioni:

a) nome e dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il nuovo regolamento introduce "Privacy by Design" che pone le basi della privacy del futuro. L'articolo 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) si esprime in tal senso:

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Ovvero la nascita del sistema di protezione avviene contemporaneamente con l'evento di rischio di cui si deve fare trattamento e quindi non si fa trattamento fintantoché l'intero sistema non è stato definito e che obbliga tutti coloro che introducono nuove rischiosità privacy sul mercato ad introdurre e certificare anche gli opportuni sistemi di sicurezza e di mitigazione del rischio.

La pseudonimizzazione dell'informazione, definita come:

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano

conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
Il medesimo articolo 25 dice anche che: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
Qui viene rappresentato il concetto di Privacy by Default dove si chiede di utilizzare il numero di informazioni necessario e sufficiente al trattamento in atto per limitare già in fase di progettazione il rischio privacy.

I registri:

Il registro del titolare del trattamento, che contiene:

- Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;
- Le finalità del trattamento;
- Le categorie degli interessati a cui fa capo il dato;
- Eventuali termini per la cancellazione automatica del dato;
- Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.
- Il registro del responsabile del trattamento, in cui sono presenti:
- L'anagrafica dei responsabili del trattamento;
- La descrizione delle categorie di trattamento effettuati;
- Opzionalmente la descrizione delle misure di sicurezza intraprese.

La conservazione può avvenire in forma cartacea ma anche in forma elettronica rendendo sempre disponibile il dato ad eventuali ispezioni dell'autorità garante.

Data Breach: violazione dei dati.

La «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Il Garante della Privacy, con attenzione anche per il nuovo GDPR, ha pubblicato gli adempimenti previsti.
In particolare vengono prese in considerazione le azioni da intraprendersi nel caso di perdita, distruzione, diffusione indebita di dati personali conservati, trasmessi o comunque trattati a causa di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi e altre calamità.

Le amministrazioni pubbliche.

In particolare il testo del nuovo regolamento prevede l'obbligo di notifica all'autorità di controllo e la comunicazione della violazione al diretto interessato.
L'articolo 33 dice infatti: Notifica di una violazione dei dati personali all'autorità di controllo:

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve:
   a. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c. descrivere le probabili conseguenze della violazione dei dati personali;
   d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo ed il 34:

- Comunicazione di una violazione dei dati personali all'interessato.

Il ruolo del Data Protection Officer:

Gli articoli 37, 38 e 39 (sezione 4) del GDPR trattano della figura del DPO (Data Protection Officer) in particolare della designazione, della posizione e dei compiti.
L'articolo 37 spiega che la figura del Data Protection Manager (DPO) non sempre è necessaria:

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
    a. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
    b. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che e, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
    oppure
    c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Compiti del responsabile della protezione dei dati

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d. cooperare con l'autorità di controllo;
e. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Normativa e ambito di utilizzo

- Legge 675/1996;
- D.P.R. 318/1999
- Legge 325/2000;
- Regolamento per l'utilizzo della rete;

- Pareri vincolanti Garante della Privacy; Normativa vigente.
- D.M. n. 305 del 7.12.2006, Regolamento concernente l'"identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal MPI, in attuazione dell'art. 20 e 21 del decreto legislativo 30.6.2003 n. 96 (il «Codice in materia di protezione dei dati personali»)";
- REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Il Parlamento Europeo e Il Consiglio dell'unione Europea:

- visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, vista la proposta della Commissione europea, previa trasmissione del progetto di atto legislativo ai parlamenti nazionali;
- visto il parere del Comitato economico e sociale europeo;
- visto il parere del Comitato delle regioni;
- deliberando secondo la procedura legislativa ordinaria;
- considerando quanto segue: La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche. La direttiva 95/46/CE del Parlamento europeo e del Consiglio ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

L'ISTITUTO

L'Istituto Tecnico Agrario Garibaldi di Roma prende origine dalla Scuola Podere che, per iniziativa del Comizio Agrario, venne aperta in Valmontone, con il concorso dei Ministero per l'Agricoltura e delle Amministrazioni Provinciale e Comunale di Roma, nell'anno 1872.
Verso la fine del 1875, la scuola fu trasferita in Roma nel Casale di S. Pio V, villa di proprietà del Principe Corsini sito sul Gianicolo, tra Porta San Pancrazio e Porta Cavalleggeri.
Nel 1882 la Scuola Podere venne trasformata in Scuola Pratica dì Agricoltura e cessò ogni dipendenza amministrativa dal Comizio Agrario. Successivamente, con la legge del 6 giugno del 1885, (che metteva ordine in tutte le iniziative inerenti l'istruzione agraria) la Scuola Pratica di Agricoltura di Roma passò alle dipendenze dei Ministero dell'Agricoltura, Industria e Commercio, cessando di essere così un ente scolastico autonomo.
Nel 1907 la Scuola fu sistemata in via provvisoria in alcuni locali della Tenuta di S. Alessio sulla via Ardeatina, sede nella quale si trova ancora oggi.
Con la deliberazione del 22 maggio 1923 la Regia Commissione approvava il progetto di costruzione di un fabbricato per la Scuola Convitto nella Regia Scuola Pratica di Agricoltura di Roma. Il fabbricato della Scuola Convitto è stato realizzato sopra un'altura sita quasi al centro della tenuta e venne consegnato nel 1928.
Nell'ottobre 1933, con la legge 15 giugno 1931 n. 889, la Scuola pervenne all'attuale ordinamento di Istituto Tecnico Agrario.
Ancora oggi l'Istituto è ubicato in Via Ardeatina n. 524, tra Via di Grotta Perfetta e Via di Vigna Murata, è dotato di Convitto maschile con relativa mensa scolastica e di Azienda Agraria di circa 67 ettari destinata a laboratorio didattico per gli allievi.

ORGANIGRAMMA

Dirigente Scolastico: Prof.ssa Patrizia MARINI
I° Collaboratore del Dirigente Scolastico: Prof. Kiumars FOROGHI BILAND
II° Collaboratore del Dirigente Scolastico: Prof. ssa Manuela CASCIANELLI
Staff del Dirigente Scolastico: Prof.ssa Cinzia AZZARETTO; Prof.ssa Cecilia BOTTINO; Prof.ssa Federica CONSOLINI; Prof.ssa Roberta D'AGOSTINO.

Il personale dipendente della scuola, docenti, ATA, assistenti specialistici e tutti gli alunni, sono tenuti al rispetto delle disposizioni inserite nel presente documento.
Utilizzando le applicazioni della rete informatica dell'Istituto, l'utente (personale docente, ATA, alunni, personale esterno) acconsente al monitoraggio delle attività svolte.

Si ricorda che l'uso delle applicazioni deve essere limitato al solo scopo lavorativo. L'uso non autorizzato delle applicazioni può essere oggetto di sanzioni amministrative e/o penali.
Lo scopo di questo documento è rendere noto le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dell'ITA"Giuseppe GARIBALDI", previsti dal Provvedimento del 25/6/2009, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici e del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Obiettivi principali:

- minimizzare il rischio di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature e/o archivi informatici e/o cartacei contenenti dati sensibili;
- minimizzare il rischio di accesso, non autorizzato alle informazioni sensibili;
- minimizzare il rischio che i dati sensibili siano modificati senza autorizzazione.

Il presente Documento Programmatico sulla Sicurezza viene divulgato a tutti gli studenti e a tutti i dipendenti della Scuola attraverso la pubblicazione sul sito web dell'Istituto http://www.itasgaribaldi-roma.gov.it
Gli Istituti scolastici si trovano di fronte a rilevanti cambiamenti che stanno interessando ed interesseranno il sistema informativo del MIUR.
L'informazione componente fondamentale per l'attività di ogni istituzione deve essere adeguatamente protetta. La sicurezza informatica protegge l'informazione nei confronti di un'ampia gamma di attacchi potenziali, al fine di garantire la continuità delle attività.

I rischi:

Rischi esterni

- Accessi non desiderati: la connessione permanente ad Internet sottopone alla possibilità di accessi alla rete interna da soggetti estranei e non autorizzati, esponendo le postazioni di lavoro e i dati in esse contenuti a rischio di manomissione o sottrazione;
- Virus: la navigazione Internet e ed il servizio di posta elettronica sono i principali veicoli di diffusione dei virus. I rischi connessi al contagio da virus informatico sono la perdita dei dati, l'accesso agli stessi da parte di soggetti estranei e non autorizzati, il blocco dei PC o di altri dispositivi connessi alla rete, il sovraccarico della stessa;
- E-MAIL Spamming: con questo nome si intendono le problematiche legate alla ricezione di un traffico di e-mail fasulle, non richieste e non sollecitate; tale rischio se non gestito può provocare:
  1. blocco dei server di posta elettronica
  2. aumento del traffico di rete e relativo sovraccarico con rallentamento delle applicazioni e relativi disservizi;
- Intercettazione dei dati: i dati trasmessi da un PC prima di giungere a destinazione attraversando la rete Internet, per definizione pubblica e non protetta, vengono gestiti da diversi apparati. Esiste quindi la possibilità che i dati vengano intercettati lungo il cammino e modificati oppure soltanto letti, con evidente violazione della privacy e dell'integrità degli stessi.

Rischi interni

- Trasmissione illecita di dati attraverso Internet a soggetti non autorizzati a ricevere/manipolare quei dati;
- Navigazione su siti Internet con contenuti non pertinenti con l'attività lavorativa.
- Traffico non consentito. La navigazione può interferire con le attività istituzionali: lo scarico/scambio di immagini, di file musicali e video, attraverso i così detti meccanismi di peer to peer.
- Manomissione, danneggiamento di sistemi, apertura di back door. Qualora il personale deputato all'amministrazione dei sistemi lasci la scuola sarà necessario revocare immediatamente tutte le autorizzazioni e provvedere alla generazione di nuovi account.

L'organizzazione per la sicurezza

La tecnologia da sola non è sufficiente. Un punto di riferimento in materia è costituito dalla direttiva del Ministro per l'Innovazione del 16 gennaio 2002 in materia di sicurezza. Essa prevede e descrive le attività per un livello di sicurezza individuato come base minima, da cui partire per ottenere miglioramenti.
La direttiva suggerisce i seguenti passi:

- definizione delle strategie generali;
- formalizzazione delle procedure e delle regole;
- controllo del rispetto delle norme;
- gestione dei problemi di sicurezza;

Le contromisure di tipo tecnico
Firewall - Antivirus Gateway - Sistema Antivirus - URL Filtering - VPN (Virtual Private Network)

Definizioni e Responsabilità

- □ Dati Identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.
- □ Dati Personali: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente.
- □ Dati Anonimi: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.
- □ Dati Sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- □ Dati Giudiziari: i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, imputato o di indagato di procedura penale.
- □ Interessato: il soggetto al quale si riferiscono i dati personali.
- □ Titolare Del Trattamento Dei Dati: il titolare del trattamento è l'istituto scolastico e la titolarità è esercitata dal Dirigente Scolastico. Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte del Responsabile delle proprie Istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- □ Titolare del trattamento dei dati dell'ITA "Giuseppe GARIBALDI" è il Dirigente Scolastico Prof.ssa Patrizia Marini
- □ Supervisor del Sistema Informatico: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico dell'ITA "Giuseppe GARIBALDI" e di consentirne l'utilizzazione.
- □ Supervisor del sistema informatico dell'ITA "Giuseppe GARIBALDI" è il Prof. Daniele Impellizzeri (Assistenza sito web, assistenza laboratori, WiFi LIM, assistenza segreteria, amministrazione di sistema).

Responsabile del Trattamento dei Dati:
Il responsabile è un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.
Responsabile del trattamento dei dati dell'ITA "Giuseppe GARIBALDI" è il Direttore S.G.A. Pietro Lauri.

□ ***Incaricato al Trattamento dei Dati***: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. Incaricati del trattamento dei dati dell'ITA "Giuseppe GARIBALDI" sono:

- tutti gli Insegnanti;
- tutti gli Educatori;
- tutti gli Assistenti amministrativi;
- tutti gli Assistenti tecnici;
- tutti i Collaboratori scolastici.
- Tutti gli Assistenti specialistici.

Amministratore del Sistema Informatico e del Dominio

L'Amministratore del Sistema Informatico provvede:

- al funzionamento della rete, comprese le apparecchiature di protezione (firewall, proxy server, filtri per la posta elettronica, antivirus, ecc.);
- a monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica;
- ad effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- a collaborare con l'amministratore della rete informatica rete uffici dell'istituto, con il custode delle password e con il responsabile del trattamento dei dati personali (D.S.G.A.)
- a collaborare con gli assistenti tecnici dell'ITA "G. GARIBALDI" a cui è stata assegnata la password con privilegi di amministratore di dominio della rete informatica didattica/laboratori di ogni sede /Convitto/Azienda;

L'Amministratore del Dominio provvede:

- al funzionamento della rete informatica con particolare attenzione al controllo della sicurezza, alla gestione e alla configurazione delle reti uffici segreteria e didattica/laboratori e degli apparati di rete;
- alla gestione e all'archiviazione dati,
- a definire le modalità di monitoraggio della funzionalità e stabilità della rete e controlla le procedure relative alla sicurezza, salvataggio e riservatezza dei dati;

- all'attività del personale tecnico interno ed esterno che interviene sulla rete;
- ad informare il Titolare del Trattamento dei dati su eventuali incidenti;
- effettua le copie di backup e di recupero dei dati (restore);
- agli aggiornamenti degli applicativi sia sul server sia sui personal computer degli uffici;
- a collaborare con i responsabili del trattamento dei dati delle sedi /Convitto/Azienda;

Nello svolgimento delle funzioni, qualora sia necessario, il gestore può avvalersi di personale tecnico per lo svolgimento di attività informatiche che richiedono complesse conoscenze e capacità.
L'amministratore di dominio del sistema informatico dell'ITA "G. GARIBALDI" è il Prof. Daniele Impellizzeri.

Custode delle password

Il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.
Custode delle password dell'ITA "G. GARIBALDI" è il Dirigente Scolastico Prof.ssa Patrizia Marini.

L'attuale configurazione della rete informatica dell'ITA "G. GARIBALDI" prevede n. 2 server:
n. 1 Server dati custodito in Vicepresidenza (I° piano) (per amministrazione e rete Lan)
n. 1 Server wi-fi in Stanza del DSGA.

L'edificio scolastico dell'ITA "G. GARIBALDI" è cablato e la configurazione della rete si suddivide in:
n. 1 rete per uffici
n. 1 rete per laboratori e per registro elettronico
n. 1 rete per il Convitto

Il Provider dei servizi dell'ITA "G. GARIBALDI" è attualmente fornito da fastweb.

Sicurezza Base Dati Utenti

La base dati utenti viene mantenuta sicura attraverso una unità di backup che effettua la copia giornaliera di backup del database utenti.
La intranet dell'Istituto scolastico si sviluppa esclusivamente su reti private. In ogni punto di interconnessione tra reti pubbliche e private è posizionato un firewall.
L'accesso ai sistemi operativi dei firewall dall'esterno è consentito solo ed esclusivamente attraverso canali sicuri.

Unità Di Backup

Il BACKUP, depositato sul NAS, è effettuato dal server giornalmente per il backup dei dati sensibili e della struttura di active directory (database di tutti gli utenti e/o oggetti presenti nel sistema). Sarà cura del Direttore S.G.A. garantire il recupero dei dati (disaster recovery) – ove necessario - attraverso l'Amministratore del Sistema incaricato anche di verificarne la correttezza della procedura.
Sistema Antivirus/Antispyware
Nella rete informatica dell'Istituto è installato un software antivirus/antispyware su tutti i pc e server degli uffici in grado di prevenire attacchi di virus informatici.

Policy

Gli utenti dell'ITA "G. GARIBALDI" non devono usare la rete per:
uso diverso da quello lavorativo; giocare in borsa; visitare siti pornografici; scommettere e fare giochi di azzardo; inserire nella "rete" dati sensibili e/o dati personali; eseguire tentativi di Port Scanning / Brute Force / Denial of Service; scaricare e diffondere programmi e/o file peer to peer; utilizzare social network (facebook, messanger, twitter, net log, ecc…) per uso non didattico; scaricare, diffondere e utilizzare software per il controllo remoto dei pc; caricare sui computer e computer dei LIM e sulla rete copie di opere protette dai diritti di copyright.
L'ITA "G. GARIBALDI" rispetta il diritto d'autore di tutti coloro che sono coinvolti nella creazione e distribuzione di musica, film, software, opere letterarie, opere d'arte e lavori scientifici.
Gli utenti dell'ITA "G. GARIBALDI" non possono scaricare, caricare, condividere, detenere e rendere disponibili copie non autorizzate di opere tutelate da diritto d'autore tramite la rete, i computer e ogni altro apparato informatico di proprietà della scuola.

Sito Web

Nel sito http://www.itasgaribaldi-roma.gov.it sono inserite le comunicazioni in base alla normativa vigente (albo on line, amministrazione trasparente, ecc…), le circolari, gli avvisi, le comunicazioni riguardanti il personale Docente, A.T.A. e alunni.

Titolare – Responsabili - Incaricati

Titolare del trattamento: Dirigente Scolastico Prof.ssa Patrizia Marini
Responsabile del trattamento dei dati: Direttore S.G.A. Pietro Lauri.
Supervisore del sistema informatico: Prof. Daniele Impellizzeri
Amministratore dei domini del sistema informatico: Prof. Daniele Impellizzeri
Amministratore esterno del sistema informatico: Prof. Daniele Impellizzeri
Amministratori di dominio della rete didattica/laboratori di sede: Prof. Daniele Impellizzeri
Responsabile gestione proxy server: Prof. Daniele Impellizzeri
Responsabile attuazione delle disposizioni contenute nel Documento Programmatico sulla Sicurezza: Prof. Daniele Impellizzeri
Custode delle password: Dirigente Scolastico Prof.ssa Patrizia;
Incaricati del trattamento dei dati: tutti gli insegnanti e gli assistenti specialistici, gli assistenti amministrativi, gli assistenti tecnici e i collaboratori scolastici;

Analisi dei rischi

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in:
rischio fisico
rischio logico
Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

Rischio Fisico

Il furto o il danneggiamento degli archivi, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre l'istituto "Giuseppe Garibaldi" al rischio di violare la legge 675/96 e successive modifiche
Archivi Cartacei
Gli archivi cartacei sono conservati nell'archivio in armadi e in locale chiuso a chiave ed appositamente predisposto e dotato di impianto antincendio.
I rischi fisici a cui sono sottoposti sono i seguenti:
Accesso agli uffici e agli archivi di persone esterne alla Scuola;
Smarrimento per incuria da parte del personale;

Furto;

Visura e/o copiatura da parte di personale non autorizzato;
Perdita parziale o totale a causa di incendi o allagamenti;
Perdita parziale o totale per il degrado naturale del supporto (invecchiamento);
Atti di vandalismo

Archivi informatici

Gli archivi informatizzati risiedono su n. 1 Server e i rischi fisici a cui sono soggetti sono i seguenti:
Distruzione fisica del server per eventi esterni allo stesso quali incendi, allagamenti, sbalzi e assenza prolungata di corrente;
Guasti hardware del server tali da impedire il recupero degli archivi che si trovano sugli hard disk;
Furto del server e/o dei supporti di backup dei dati;
Perdita di dati dovuta a imperizia del personale addetto;
Accesso ai server da parte di personale non autorizzato;

Atti di vandalismo.

I locali che contengono apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari, archivi informatici e dispositivi di copia), e/o gli archivi cartacei contenenti dati sensibili dell'Istituto "Giuseppe Garibaldi" sono situati in locali ad accesso controllato all'interno di aree sotto la responsabilità dell'ITA "G. GARIBALDI"; i responsabili dei trattamenti sono anche responsabili dell'area in cui si trovano i trattamenti; i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura dei collaboratori scolastici addetti

alla reception; l'ingresso ai locali ad accesso controllato è è consentito solo alle persone autorizzate ed è possibile solo dall'interno dell'area sotto la responsabilità dell'ITA "G. GARIBALDI, i locali sono provvisti di estintore.

I rischi e le minacce interne ed esterne cui sono soggetti gli archivi informatici possono inoltre essere i seguenti:

- rischio interno all'organizzazione relativo all'utilizzo della LAN/Intranet;
- utilizzo di pen drive non opportunamente verificate circa la presenza di software maligno;
- accesso alle banche dati da parte di personale esterno alla Scuola;
- accesso alle informazioni da parte di personale non autorizzato attraverso i punti di contatto con il mondo esterno (INTERNET);
- rischio esterno dovuto ad intrusioni nel sistema da parte di hacker;
- rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser;
- rischio interno dovuto a intrusioni da parte di personale docente, ATA e studenti.
- minaccia alla proprietà/confidenzialità/autenticità dell'informazione
- cattura di password (sniffers, trojan horse, worm, IP spoofing, brute force, password cracking, packet sniffing, port scanning, highjacking, social engineering, buffer overflow, logic bomb, malware e MMC (Malicious Mobile Code), DoS (Denial of Service), DDOS (Distributed Denial of Service);
- acquisizione dei privilegi di amministratore di sistema da parte di soggetti non autorizzati;
- mail spamming (utilizzo dei server di posta elettronica per la spedizione su Internet di messaggi non richiesti, ad esempio pubblicitari)
- minaccia all'integrità dell'informazione: diffusione di virus informatici (application-layer attacks):
- minaccia alla disponibilità dell'informazione: denial-of-service (fermo dei servizi, fermo macchina, distruzione di dati).

Le principali minacce alle risorse hardware sono:

malfunzionamenti dovuti a guasti; malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi; malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica; malfunzionamenti dovuti a sabotaggi, furti.

Le principali minacce ai dati trattati sono:

accesso non autorizzato agli archivi contenenti le informazioni riservate da parte di utenti interni e/o esterni; modifiche accidentali agli archivi da parte di utenti autorizzati.

Le principali minacce ai supporti di memorizzazione sono:

distruzione e/o alterazione a causa di eventi naturali; imperizia degli utilizzatori; sabotaggio; deterioramento nel tempo (invecchiamento dei supporti); difetti di costruzione del supporto di memorizzazione che ne riducono la vita media; l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Tabella dei RISCHI:

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Allagamento	X	X	X
Uragani / Fulmini			X
Incendio	X	X	
Vandalismo	X		
Blackout / Interruzione fornitura		X	
Arresto condizionatori	X	X	
Guasto hardware		X	
Instabilità tensione elettrica / Scariche elettrostatiche		X	X
Sbalzi Temperatura		X	X
Polvere			X
Radiazioni elettromagnetiche		X	

Furto	X		
Uso non autorizzato apparati e strumenti	X		
Danneggiamento dei supporti di memoria	X	X	
Errore del personale / Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software e/o dannoso	X	X	
Accesso e uso non autorizzato alla rete /	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione	X		
Analisi del traffico	X		
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Blocco software	X	X	
Uso di software da parte di non autorizzati	X	X	

Analisi dei rischi

EVENTO		**IMPATTO SULLA SICUREZZA DEI DATI**		**RIF. MISURE DI AZIONE**
		DESCRIZIONE	**GRAVITÀ STIMATA**	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	**M**	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	**M**	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	**M**	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;	**EE**	Adozione di idonei dispositivi di protezione
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**EE**	Adozione di idonei dispositivi di protezione

	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**MA**	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**MA**	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	**MA**	Adozione di idonei dispositivi di protezione
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	**MA**	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	**M**	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**A**	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.

Sulla scorta della ricognizione dei rischi sopra rappresentata, l'istituzione scolastica ha provveduto ad apprestare e/o introdurre strumenti di tutela, ovvero a prevedere successive, e più incisive, misure di sicurezza. La tabella seguente sintetizza le misure di sicurezza in essere, corredate da indicazioni di dettaglio.

Tabella: Le misure di sicurezza adottate o da adottare

MISURA	RISCHIO CONTRASTATO	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIÀ IN ESSERE	PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria/ Dirigente scolastico	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Mensile; Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Ufficio personale	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Mensile; Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi amministrativi	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Mensile; Responsabile pro tempore*:* Prof. Daniele Impellizzeri
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi inerenti l'offerta formativa	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Mensile; Responsabile pro tempore: Prof. Daniele Impellizzeri
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi strumentali agli organi collegiali	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Mensile; Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri

Data					

Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati. Sono state perciò acquisite licenze di uso per software antivirus, nonché sistemi di firewall con verifica di idoneità e costante aggiornamento. In ogni caso si osserva che l'istituzione scolastica dispone di un sistema di controllo degli accessi ai locali. I documenti sono anche conservati in copia cartacea presso locali dell'istituzione scolastica non accessibili ai terzi e dotati di adeguati strumenti di protezione (armadi con serrature).

Sinteticamente è possibile rappresentare la seguente procedura di copia, verifica e ripristino dei dati per ogni p.c. o terminale di collegamento a server

Tabella: Procedure di copia, verifica e ripristino per ogni singola unità contenente dati

Struttura in possesso di p.c. o collegamento a server	Applicativo	Sistema operativo	Supporti magnetici	Procedura di copia	Procedura di verifica	Ripristino
Segreteria/ Dirigente scolastico	Office- Axios - ClasseViva	Server Windows 2008 e Windows 7	HD, PenDrive - usb	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale
Ufficio personale	Office –Sissi – Axios – Classe Viva	Server Windows 2008 e Windows 7	HD, PenDrive - usb	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale
Servizi amministrativi	Office-Sissi – Axios - Classe Viva	Server Windows 2008 e Windows 7	HD, PenDrive - usb	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale	Procedura di backup Server Windows 2008 e Windows 7 giornaliero e settimanale
Servizi inerenti l'offerta formativa	Office- Axios – Classe Viva	Server Windows 2008 e Windows 7	HD, PenDrive - usb	Procedura di backup Windows e server	Procedura di backup Windows e server	Procedura di backup Windows e server
Servizi strumentali agli organi collegiali	Office- Axios– Classe Viva	Server Windows 2008 e Windows 7	HD, PenDrive - usb	Procedura di backup Windows e server	Procedura di backup Windows e server	Procedura di backup Windows e server
Data						

Con riferimento invece al contenuto ed alle competenze in tema di copia, verifica e ripristino, le soluzioni organizzative adottate presso l'istituzione scolastica sono sintetizzate nella seguente tabella:

Tabella: Salvataggio dei dati

SALVATAGGIO		CRITERI INDIVIDUATI PER IL SALVATAGGIO	UBICAZIONE DI CONSERVAZIONE DELLE COPIE	STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO
STRUTTURA	DATI SENSIBILI O GIUDIZIARI CONTENUTI			
Segreteria Dirigente scolastico	Protocollo riservato- dati giudiziari	Salvataggio dati periodico	Locale in sede sito al piano terra nell'ufficio di Presidenza con serratura con chiavi distribuite ai soli autorizzati	Responsabile servizio: Dirigente e Prof. Daniele Impellizzeri
Ufficio personale	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati giornaliero su server e periodico sui PC	Locale server in sede con serratura con chiavi distribuite ai soli autorizzati	Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri
Servizi amministrativi	Dati inerenti l'azienda, i fornitori, e servizi cassa per ministero	Salvataggio dati giornaliero su server e periodico sui PC - archivio cartaceo	Locale server in sede sito al piano terra nell'ufficio di Presidenza con serratura con chiavi distribuite ai soli autorizzati	Responsabile pro tempore del servizio dati su server: Prof. Daniele Impellizzeri; Responsabile archivi cartacei il DS e il DSGA
Servizi inerenti l'offerta formativa	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati giornaliero su server e periodico sui PC	Locale in sede con serratura con chiavi distribuite ai soli autorizzati	Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri
Servizi strumentali agli organi collegiali	- Stato di salute - origine razziale o etnica -confessione religiosa	Salvataggio dati giornaliero su server e periodico sui PC	Locale in sede con serratura con chiavi distribuite ai soli autorizzati	Responsabile pro tempore del servizio: Prof. Daniele Impellizzeri
Data:				

Con riferimento alle procedure di ripristino, l'Istituzione scolastica ha adottato le seguenti modalità

Ripristino dei dati

RIPRISTINO (in seguito a distruzione o danneggiamento)		
DATA BASE/ARCHIVIO	SCHEDA OPERATIVA	PIANIFICAZIONE DELLE PROVE DI RIPRISTINO
Segreteria (personale, amministrativa, didattica)	Viene effettuato in automatico dal sistema un backup dei dati trattati e dei documenti presenti sull'HD sul NAS localizzato all'interno della sede dell'istituzione scolastica "G. GARIBALDI" di Roma e precisamente nella segreteria del D.S.G.A.	Trimestrale

Tabella: Trattamenti affidati all'esterno

ATTIVITÀ COMPORTANTE TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI DESCRIZIONE SINTETICA DATI PERSONALI, SENSIBILI O GIUDIZIARI INTERESSATI	SOGGETTO	DESCRIZIONE DEI CRITERI PER L'ADOZIONE DELLE MISURE

Conservazione e messa a disposizione tramite server in dotazione delle informazioni occorrenti per lo svolgimento dei compiti d'ufficio necessario per lo svolgimento delle attività strumentali finalizzate all' installazione e al buon funzionamento degli elaboratori, dei programmi e degli altri strumenti elettronici in dotazione agli uffici.	Amministratore di Sistema di cui al contratto Prot.n.7460/4.1.p del 2018.	Vincolo contrattuale, a carico dell'Amministratore di Sistema, a tenere i comportamenti descritti in calce alla presente tabella.

Vincoli Contrattualmente Assunti dall'Amministratore di Sistema ai Fini della Sicurezza dei Dati

L'Istituzione scolastica ha affidato all'Amministratore di Sistema, nei termini risultanti dalla sopraindicata tabella, i trattamenti di dati personali sensibili o giudiziari, effettuato con strumenti elettronici, previa assunzione da parte dell'affidatario – nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo – degli impegni derivanti dalle seguenti dichiarazioni:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Elenco dei trattamenti: informazioni essenziali

Descrizione sintetica del trattamento			Natura dei dati		Struttura di riferimento	Altre strutture che concorrono al trattamento
Finalità perseguita o attività svolta	Categorie di interessati	Terzi a cui vengono comunicati i dati	S	G		
Gestione Area Alunni Relativamente ai dati sensibili e giudiziari: Attività propedeutiche all'avvio dell'anno scolastico; Attività educativa, didattica e formativa e di valutazione; Rapporti Scuola-Famiglie: gestione del contenzioso.	Alunni Genitori	USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi di polizia giudiziaria,	S	S	DIDATTICA COMM. FORMAZIONE CLASSI COORDINATORI	UFF. PROTOCOLLO UFFICIO PERSONALE
Gestione Area Bilancio	Personale Fornitori	USP, USR, MPI, Agenzia delle Entrate, Altre istituzioni scolastiche, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Banca che effettua il servizio di cassa			AMMINISTRAZIONE DIDATTICA	UFF. DSGA

Gestione Area Personale Relativamente ai dati sensibili e giudiziari : Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Gestione del contenzioso e procedimenti disciplinari; Organismi collegiali e commissioni istituzionali; Rapporti Scuola-Famiglie: gestione del contenzioso.	Personale	USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego	S	S	UFF PERSONALE PROTOCOLLO AMMINISTRAZIONE	UFF. DSGA
Gestione Area Retribuzioni Relativamente ai dati sensibili e giudiziari : Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Gestione del contenzioso e procedimenti disciplinari; Organismi collegiali e commissioni istituzionali;	Personale	USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Magistrature ordinarie e amministrativo-contabile, Agenzia delle Entrate, Banca che effettua il servizio di cassa	S	S	AMMINISTRAZIONE PERSONALE	UFF. DSGA
Gestione Fiscale	Personale	USP, MPI, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, MEF, Banca che effettua il servizio di cassa			AMMINISTRAZIONE	UFF. DSGA UFFICIO PERSONALE
Gestione Protocollo Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, Genitori, Fornitori, Personale, Altre amministrazioni	USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa	S	S	PROTOCOLLO	DIDATTICA AMMINISTRAZIONE UFF. DSGA
Backup e Restore	Banca dati Amministrativa				DITTA ESTERNA	

Gestione Protocollo e corrispondenza riservata Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, genitori, personale	USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Organi di polizia giudiziaria	S	S	PROTOCOLLO DS DSGA	DS
Gestione della posta elettronica	Personale, utenti del servizio scolastico, fornitori				PROTOCOLLO	DS DSGA
Gestione Scioperi del Personale dipendente Relativamente ai dati sensibili e giudiziari : Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;	Personale	https://websptnet.tesoro.it/	S		PERSONALE PROTOCOLLO	DSGA
Gestione Anagrafe delle prestazioni	Personale interno ed esterno, Fornitori	www.anagrafeprestazioni.it			PERSONALE	DSGA
Gestione INPS	Personale	INPS	S		PERSONALE	DSGA
Gestione con Suite Microsoft Office comunicazione	Personale interno ed esterno, Fornitori				Tutte	Tutte
Gestione Dispostivi dell'infrastruttura tecnologica	Personale interno ed esterno, Fornitori				ASSISTENTI TECNICI DITTA ESTERNA	
Gestione Provvedimenti Disciplinari alunni Relativamente ai dati sensibili e giudiziari : Attività propedeutiche all'avvio dell'anno scolastico; Attività educativa, didattica e formativa e di valutazione; Rapporti Scuola-Famiglie: gestione del contenzioso.	Genitori, Alunni, Personale	Genitori, USP	S		DIDATTICA COORDINATORI DI CLASSE VICEPRESIDENZA	DS DSGA

Gestione Graduatorie e supplenze	Personale	USP, USR, MPI			PERSONALE COMM. GRADUATORIE	DSGA
Gestione del personale	Personale		S	S	PERSONALE	DS DSGA
Gestione Area e Contratti prestazione	Personale interno ed esterno Alunni	Enti Pubblici Territoriali, INAIL, Organizzazioni Sindacali, Ditte Esterne			DS DSGA	
Gestione Trattative sindacali Relativamente ai dati sensibili e giudiziari - Organismi collegiali e commissioni istituzionali;	Contrattazione sindacale	Componenti RSU Organizzazioni Sindacali	S		DS DSGA	
Gestione Archivio cartaceo storico	Tutte le categorie	I dati non vengono comunicati a terzi (prima dell'eventuale comunicazione vengono trasferiti alle strutture interne autorizzate al trattamento)	S	S	UFFICI DI SEGRETERIA	
Gestione Assistenza e manutenzione hardware	Tutti i soggetti che utilizzano i PC degli uffici Amministrativi				DITTA ESTERNA	
Gestione Riproduzione e notifica documenti	Personale, Alunni, Genitori Fornitori				PERSONALE PROTOCOLLO	UFF. DSGA
Gestione Atti cartacei amministrativi	Personale, Alunni, Genitori Fornitori				PERSONALE-AMMINISTRAZIONE DIDATTICA	DSGA
Gestione Inventario e Fornitori di beni e servizi	Ditte esterne	Ditte esterne			AMMINISTRAZIONE	DS DSGA

Atti e Documenti non in Formato Elettronico, Archivi Cartacei

I trattamenti di dati personali con strumenti diversi da quelli elettronici sono effettuati dagli incaricati seguendo le istruzioni scritte ad essi impartite con il documento di cui all'allegato 1, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ha carattere annuale. Gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solamente alle persone preventivamente autorizzate.

Contromisure

Individuazione delle contromisure adottate

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

1. contromisure di carattere fisico;
2. contromisure di carattere procedurale;
3. contromisure di carattere informatico.

Contromisure di carattere fisico

Gli archivi cartacei e le apparecchiature informatiche critiche contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato; i locali ad accesso controllato sono all'interno di aree sotto la responsabilità dell'ITA "G. GARIBALDI"; i responsabili dei trattamenti sono anche responsabili dell'area in cui si trovano i trattamenti; i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura dei collaboratori scolastici addetti alla reception; l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ITA "G. GARIBALDI, i locali sono provvisti di estintore.

Contromisure di carattere procedurale

- l'ingresso nei locali è controllato ed è consentito solo alle persone autorizzate;
- i visitatori occasionali sono identificati e accompagnati da un incaricato;
- per l'ingresso è necessaria preventiva autorizzazione da parte del DS o del Primo Collaboratore.
- è attuato la verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso negli uffici da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i dati sono inaccessibili e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri di classe, contenenti dati comuni e particolari (certificati medici esibiti dagli alunni a giustificazione delle assenze), durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono dall'insegnante dell'ultima ora di lezione conservati, per la loro custodia, in apposito armadio dotato di serratura nella stanza individuata come sala docenti.
- il docente è responsabile della riservatezza del registro personale (Classe viva) in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il tablet per il registro viene conservato nell'armadietto del docente che è chiuso a chiave. Una chiave di riserva è mantenuta con le dovute cautele dalla scuola (presso l'ufficio Personale);
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato presso la cassaforte nell'ufficio del D S..
- è fatto divieto di fare fotocopie e/o fare scansioni di documenti senza l'autorizzazione del responsabile del trattamento;
- è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'Istituto senza l'autorizzazione del responsabile del trattamento, tale divieto si estende anche all'esportazione telematica; il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

Le misure di carattere informatico adottate sono:

- utilizzo di server con configurazioni di mirroring;
- presenza di gruppi di continuità elettrica per il server ubicato uno in sede centrale;
- definizione delle regole per la gestione delle password;
- definizione delle regole per la gestione di strumenti informatici;
- definizione delle regole di comportamento per minimizzare i rischi da virus;
- separazione fisica e logica della rete locale delle segreterie da quella dei laboratori didattici per mezzo di USERNAME/password.

Sicurezza fisica dei computer

I server dove sono presenti il database e l'active directory di tutti gli utenti ed il web server della scuola sono situati nell'ufficio tecnico ad accesso controllato e in appositi armadi chiusi a chiave.

Difesa da accessi non autorizzati da rete geografica

Tutti gli assistenti amministrativi che utilizzano i software gestionali accedono al sistema informativo per mezzo di USERNAME e password personale. La password è assegnata dal Direttore S.G.A. che assegna inoltre le aree di competenza (p.es. alunni, bilancio, magazzino, inventario, conti correnti, protocollo, carriera,…) e i relativi diritti (lettura, scrittura). USERNAME e password sono strettamente personali e non possono essere riassegnate ad altri utenti. L'elenco delle password è conservato in cassaforte.

Ai sensi dell'Allegato B al D.Lgs. 196/2003 la password deve essere modificata almeno ogni 6 mesi. In caso di trattamento di dati sensibili, la modifica deve avvenire ogni 3 mesi.

Regole di utilizzo delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale e password personale.

User-id e password iniziali sono assegnati dall'amministratore del sistema. User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

Non è consentito trascrivere le password su supporti agevolmente accessibili da parte di terzi (post-it o altro sullo schermo o sulla scrivania); le credenziali non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; le credenziali sono disattivate anche in caso di perdita dei requisiti per poter essere utente attivo del dominio dell'Istituto.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi; l'utente è tenuto a rendere inaccessibile la propria postazione di lavoro ogni volta che si assenta, utilizzando la funzione di blocco del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca computer").
La password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC e dei firewall che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
La password è un elemento fondamentale per la sicurezza delle informazioni.
La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.
Le credenziali sono disattivate anche in caso di perdita di qualità che consente all'utente l'accesso caso di trattamento di dati sensibili, la modifica deve avvenire ogni 3 mesi.
Protezione degli archivi informatici
I server che ospitano gli archivi con dati sensibili utilizzano le seguenti regole: obbligo di password di BIOS; autorizzazione scritta per l'accesso agli incaricati ed agli addetti alla manutenzione; gli hard disk non devono essere condivisi in rete; supervisione dell'incaricato del trattamento a tutte le operazioni di manutenzione che devono essere effettuate on-site; antivirus costantemente aggiornato; backup proceduralizzato concordato con i responsabili del trattamento e del sistema informatico; conservazione in cassaforte delle copie di backup; obbligo di uso di screen saver con password; divieto di installazione, sui PC, di archivi con dati sensibili di carattere personale dell'utente; divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati; divieto di installazione sui personal computer che contengono archivi con dati sensibili accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.
Al gestore del sistema informatico competono tutte le operazioni connesse al salvataggio giornaliero, settimanale, mensile e annuale dei dati del database
Le operazioni di Restore sono affidate al Prof. Daniele Impellizzeri che presta consulenza e assistenza tecnica, le copie delle password, degli user id e dei backup dei dati sono custodite dal Dirigente Scolastico e dal Direttore S.G.A.
Gli hard disk non più utilizzabili devono essere distrutti meccanicamente alla presenza dell'incaricato del trattamento;
Gli hard disk ancora idonei all'uso, come nel caso di sostituzioni o dismissioni di personal computer, dovranno essere sottoposti a *wiping* alla presenza dell'incaricato del trattamento che dovrà accertare la reale cancellazione di tutti i dati.

Servizi

L'ITA "G. GARIBALDI" utilizza i programmi software di Spaggiari per il registro elettronico e il protocollo con "ClasseViva" e di Axios per la gestione amministrativa –finanziaria.

Struttura	***Descrizione dei compiti e delle responsabilità***

Ufficio Personale	• Uso applicativo Axios • Uso Applicativo Classe Viva (Spaggiari- Protocollo) • Gestione dei documenti office automation • Accesso all'area riservata del sito Istruzione • Accesso al servizio di gestione degli scioperi • Consultazione e archiviazione dei fascicoli personali dei dipendenti • Gestione del software per la rilevazione delle presenze del personale • Gestione della posta elettronica
Ufficio Contabilità	• Uso applicativo Axios Area contabilità • Uso Applicativo Classe Viva (Spaggiari Protocollo) • Accesso all'area del sito www.istruzione.it • Gestione dei documenti office automation • Accesso all'area riservata del sito Istruzione • Gestione della documentazione cartacea relativa al bilancio • Invio Documenti Entratel • Invio documenti PRE96 • Invio DMA
Ufficio Protocollo	• Uso Applicativo Classe Viva (Spaggiari- Protocollo) • Gestione dei documenti office automation • Accesso all'area del sito www.istruzione.it • Stampe registro protocollo • Smistamento e archiviazione corrispondenza
Organizzazione - Area amministrazione	• Gestione dei documenti office automation • Uso Applicativo Classe Viva (Spaggiari- Protocollo) • Contratti personale esterno Istituzione scolastica • Tenuta registri Corsi
Ufficio Tecnico	• Gestione dei documenti office automation • Tenuta Inventario beni • Rapporti con i fornitori • Gare e acquisti di beni e servizi
Ufficio Didattica Alunni	• Utilizzo del'applicativo Axios Area Alunni • Uso Applicativo Classe Viva (Spaggiari- Protocollo – area alunni) • Gestione dei documenti di office automation • Accesso all'area del sito www.istruzione.it • Accesso al servizio di denuncia infortuni • Consultazione e archiviazione dei fascicoli personali degli alunni
Ufficio Dirigente Scolastico	• Gestione degli Organi collegiali • Gestione dell'offerta formativa • Gestione della sicurezza sul posto di lavoro • Gestione della protezione dei dati personali • Relazioni sindacali • Rapporti con gli enti • Gestione Protocollo Riservato
Ufficio Direttore Servizi Generali e Amministrativi	• Gestione del Bilancio • Utilizzo di tutti gli applicativi Axios • Utilizzo Applicativo gestione Sicurezza • Uso Applicativo Classe Viva (Spaggiari- Protocollo) • Gestione dei documenti office automation • Accesso all'area del sito www.istruzione.it • Gestione rapporti con il personale • Organizzazione del Lavoro ATA • Concessione credenziali accesso area riservata istruzione.it
Ufficio Collaboratore del D.S.	• Gestione Provvedimenti disciplinari alunni • Rilevazione assenze alunni della scuola • Gestione dei documenti di office automation

Amministratore di Sistema	• Amministra il Server di sistema Serversissi con il Dbase SISSI e ClasseViva • Amministra i sistemi operativi dei clients in rete • Amministra e configura il router per l'accesso ad internet • Provvede agli aggiornamenti degli applicativi Axios e la loro installazione • Predispone l'automazione del backup dell'archivio SISSI con l'applicativo Axios • Installa sui client della rete amministrativa idoneo Antivirus • Installa su tutte le macchine idonei programmi antispywere • Utilizza l'applicativo Axios Gestione Sicurezza per la gestione degli accessi e dei profili
Personale Docente	• Trattamento dati degli alunni
Archivio storico	• Gestione e archiviazione Atti Amministrativi dell'Istituzione Scolastica
Personale Ausiliario	• Riproduzione mediante fotocopiatura dei documenti e notifica degli stessi

Piano di formazione

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.
- Incidente informatico

Tutti gli incaricati del trattamento dei dati sono pregati di avvisare tempestivamente il gestore del sistema informatico e i responsabili del trattamento dei dati nel caso in cui constatino le seguenti anomalie:

discrepanze nell'uso del USERNAME/password; modifica e furto di dati; cattive prestazioni del sistema; quote particolarmente elevate di tentativi di connessione falliti.
La successiva fase di indagine e di ripristino del sistema deve essere condotta da personale esperto
Il Dirigente Scolastico, il Direttore S.G.A. e i responsabili del trattamento valuteranno se coinvolgere esperti e/o autorità di polizia competenti.
E' indispensabile che, per un'eventuale indagine, venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

Verifica dell'adeguatezza delle misure di sicurezza

L'ITA "G. GARIBALDI" verifica periodicamente l'adeguatezza ed efficacia delle misure di sicurezza adottate provvedendo ad adeguare le stesse alla particolare evoluzione tecnologica del settore, al fine di mantenere elevato il livello di protezione e ridurre, quindi, il livello di rischio.
L'attività di verifica viene attuata mediante procedure di *monitoraggio* e di *audit* ed in particolare:

- attraverso un sistema di monitoraggio effettuato da responsabili interni che eseguono un controllo costante dell'effettivo funzionamento del sistema informatico e delle misure di sicurezza, adottando tutte le misure necessarie ad incrementarne il livello di efficacia;
- attraverso la previsione di un'attività di audit, quale controllo saltuario svolto da soggetti *diversi* dai responsabili interni, al fine di ottenere un giudizio imparziale circa la qualità delle misure di sicurezza approntate ed in grado di evidenziarne eventuali debolezze od errori.

Aggiornamento del piano

Il presente piano è soggetto a revisione annuale con scadenza ogni anno scolastico; resta comunque valido fino a pubblicazione della successiva revisione.

Verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati (per l'accesso ai dati utilizzati nelle operazioni di trattamento)

- Verifica dell'operato degli amministratori di dominio
- Aggiornamento del Disciplinare Interno per l'utilizzo della posta elettronica e di Internet
- Pianificazione degli interventi formativi degli incaricati del trattamento
- Aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne eventuali difetti (l'aggiornamento deve essere effettuato con cadenza semestrale in caso di trattamento di dati sensibili o giudiziari).

Adempimenti semestrali

- Aggiornamento dei software antivirus
- Cambio password (trimestrale nel caso di trattamento di dati sensibili e/o giudiziari)

Adempimenti periodici

- Disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi
- Salvataggio dei dati con frequenza almeno settimanale.

Norme per il personale

Tutti i dipendenti (Docenti, Educatori, A.T.A. e studenti) concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa nel rispetto di quanto stabilito nel presente documento, dal regolamento di utilizzo della rete e dalla normativa vigente.

Regolamento amministratore di dominio / amministratore di sistema

In data 24 dicembre 2008 è stato pubblicato sulla Gazzetta Ufficiale n. 300 il provvedimento del Garante della privacy recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008", parzialmente modificato con la comunicazione del Garante del 10/12/2009. Il provvedimento serve soprattutto a richiamare l'attenzione "sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare al titolare in caso di incauta o inidonea designazione".

I punti principali del provvedimento sono:

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, gli amministratori di sistemi

Gli amministratori di sistema così ampiamente individuati nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Tra l'altro, lo svolgimento di mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non sempre si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.

Il Codice privacy non ha incluso questa figura tra le proprie definizioni normative (al contrario degli incaricati e del responsabile del trattamento che sono figure tipizzate). Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nell'Allegato B del Codice privacy, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione.

Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia

In relazione a tali attività il Titolare del trattamento (e dunque l'istituzione scolastica attraverso il Dirigente) deve adottare opportune cautele, avendo ben presente che si tratta di un incarico a carattere fiduciario da assegnare a persona competente e affidabile. Ci sono, al riguardo, responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare dalla incauta o inidonea designazione.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema e di dominio, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza.
Qualora l'attività degli amministratori di sistema e di dominio riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, questi vanno informati attraverso gli strumenti consentiti dal Codice privacy.
L'operato degli amministratori di sistema e di dominio deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti. Devono essere adottati sistemi idonei alla registrazione degli accessi logici
(autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e di dominio. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. L'attività dell'amministratore di sistema si inquadra in due contesti:
L'attività di ordinaria amministrazione volta a garantire il normale funzionamento e lo sviluppo dei sistemi amministrati. In tal caso l'amministratore di sistema opera di concerto con l'utente, e comunque coordinandosi in via preventiva con il supervisore del sistema e/o con il gestore del sistema informatico;
La gestione delle emergenze quando si rilevino condizioni che pongano a rischio immediato la corretta funzionalità dei sistemi o della rete, o la sicurezza dei dati e dei sistemi, l'amministratore di sistema può operare in autonomia e per le vie brevi, qualora l'onere del coordinamento limiti l'efficacia e la tempestività degli interventi.
Immediatamente dopo l'intervento, è tenuto comunque a segnalare per iscritto agli utenti coinvolti e al supervisore del sistema e/o il gestore del sistema informatico i dettagli dell'evenienza occorsa.
L'amministratore di sistema deve avere ragionevole cura:

- nel prendere precauzioni contro i furti ed i danni ai componenti del sistema;
- nell'attuare rigorosamente tutti gli accordi di licenza hardware e software applicabili al sistema;
- nel trattare informazioni riguardanti gli utenti del sistema, nonché le informazioni depositate nel sistema dagli utenti medesimi, in modo appropriato, applicando rigorosamente le norme e le pratiche atte a garantire la sicurezza dei sistemi, delle reti e dei dati. Si fa particolare riferimento al caso di azioni dolose volte a violare l'integrità dei sistemi, dei dati o della privacy (ad es. intrusioni, diffusioni di virus, etc.), ed al caso di incidenti di natura tecnica (ad es. incendio, perdita di dati, etc.);
- nel diffondere informazioni sui regolamenti e le procedure specifiche che regolano l'accesso e l'uso del sistema, sui servizi forniti e su quelli esplicitamente non forniti. Un documento scritto consegnato agli utenti o messaggi inviati tramite il sistema stesso saranno considerati una notifica adeguata;
- nel collaborare con il supervisore del sistema e/o con il gestore del sistema informatico per trovare e correggere problemi causati ad altri dall'uso/abuso del proprio sistema. Un amministratore di sistema può temporaneamente interdire l'accesso e l'uso delle risorse informatiche ad un utente se, sulla base di comprovati motivi, lo ritiene necessario per garantire la sicurezza del sistema o della rete.
- Se l'amministratore di sistema ha chiare evidenze di cattivo uso delle risorse informatiche che indirizzino ad attività di elaborazione o files di uno specifico individuo, deve attuare uno o più dei seguenti passi, considerati appropriati per la protezione degli altri utenti, della rete e dei sistemi di computer:
- notificare per iscritto le eventuali indagini al supervisore del sistema e/o al gestore del sistema informatico;
- adottare tutti i provvedimenti e le azioni ritenute necessarie e/o opportune dai responsabili di cui al punto a), per inibire il propagarsi dei danni alle risorse di rete.
- In risposta alle disposizioni del garante a breve sarà installato sulla rete interna dell'istituto un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e di dominio. Le registrazioni (access log) avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un congruo periodo, non inferiore ai 6 mesi.

All'amministratore di dominio è riservata la manutenzione dei dati relativi ai servizi attivi sul dominio nel rispetto della normativa vigente.

Regolamento per l'utilizzo del sistema informatico

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica dell'ITA "G: GARIBALDI" e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. Utilizzando le applicazioni della rete informatica dell'istituto l'utente acconsente al monitoraggio delle attività svolte.

L'uso delle applicazioni deve essere limitato al solo scopo lavorativo
L'uso non autorizzato delle applicazioni può essere oggetto di sanzioni amministrative e/o penali.

Durante l'utilizzo della rete informatica dell'Istituto e accedendo a Internet dalla stessa vanno sempre rispettate tutte le disposizioni di legge, in particolare la legge n. 547 del 31/12/93 (sui crimini informatici) e il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016.
L'ITA "G. GARIBALDI" promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
E' vietato modificare la configurazione dei personal computers, LIM. E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.
L'utilizzo dei servizi della rete è autorizzato solo per scopi didattici.
È vietato danneggiare in qualunque modo l'attrezzatura utilizzata, in particolare è vietato compromettere il funzionamento della rete e degli apparati che la costituiscono con programmi (virus, worm, trojan horses, o simili) costruiti appositamente.
È vietato modificare in qualsiasi modo la configurazione fisica e logica della rete. In particolare:
è vietato modificare la configurazione TCP/IP degli elaboratori che si utilizzano;
è possibile collegare alla rete didattica "notebook" personali solo previa autorizzazione dell'amministratore di sistema / rete, che fornirà l'autorizzazione necessaria;

- è vietato collegare alla rete in qualsiasi modo elaboratori personali o altri dispositivi compresi portatili, palmari e simili;
- è vietato l'utilizzo di credenziali altrui di cui si è venuti casualmente o intenzionalmente a conoscenza.
- è vietato comunicare e diffondere i dati personali conosciuti o ai quali si abbia avuto accesso nello svolgimento delle prestazioni lavorative, se non autorizzati dal titolare del trattamento;

Sono vietati comportamenti lesivi dei diritti di altri, quali:

- archiviare, inserire, accedere, diffondere in rete dati personali (e in particolare: informazioni su gusti, opinioni politiche o religiose, fotografie) propri o di terze persone;
- violare la privacy di altri utenti, ad esempio intercettandone la posta elettronica o accedendo senza autorizzazione ai loro files/cartelle;
- violare la sicurezza di archivi e/o computer della rete;
- furto di dati e/o manomissione

In caso di manutenzioni ordinarie o straordinarie, guasti o altri problemi non è garantito il ripristino di tutte e parte delle funzionalità dei sistemi o degli account, né tantomeno il rapido intervento o il preavviso su base personale. Nessun danno diretto o indiretto sarà attribuibile alla perdita di dati o al mancato utilizzo dei servizi abitualmente disponibili. È responsabilità dei singoli utenti il salvataggio del proprio lavoro mediante copia dei file importanti.
L'accesso ai laboratori di informatica non è permesso agli allievi in assenza di un insegnante responsabile o del personale ATA incaricato della sorveglianza. I singoli alunni, possono accedere ai laboratori, esclusivamente per scopi didattici, previa autorizzazione rilasciata dal Dirigente Scolastico o dai Collaboratori del DS con la presenza di un personale ATA.
Qualunque violazione delle modalità sopra indicate viene perseguita, civilmente e penalmente.
Attività vietate (policy)
E' vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'ITA "G. GARIBALDI";
- utilizzare la rete per le scommesse e per i giochi di azzardo; utilizzare la rete con le credenziali di accesso di altri utenti e/o cedere a terzi codici personali (USERNAME e PASSWORD) di accesso al sistema;
- violare la riservatezza di altri utenti o di terzi; agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni o che ne distraggano risorse;
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;

- cancellare, disinstallare, copiare, o asportare deliberatamente database per scopi personali;
- installare, rimuovere, danneggiare componenti hardware;
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti; utilizzare Internet e la posta elettronica per scopi personali e/o inviando e ricevendo materiale che
- violi le leggi; accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione; monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare, anche in remoto, le attività degli utenti; leggere, copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete; inserire o cambiare la password del bios, se non dopo averla espressamente
- comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile;
- usare la rete a scopo diverso da quello lavorativo;
- inserire nella "rete" dati sensibili e/o dati personali;
- eseguire tentativi di Port Scanning / Brute Force / Denial of Service; scaricare e diffondere programmi, file P2P (winmx, kazaa, emule, ecc….) ed utilizzare social network (face book, messanger, net log, ecc…);
- scaricare, diffondere e utilizzare software per il controllo remoto dei pc;
- effettuare copie di backup dei database dei server contenenti dati sensibili; caricare sui computer e sulla rete copie di opere dell'ingegno protette. Allo stesso modo, tali opere non possono essere distribuite tramite internet e gli utenti non sono autorizzati ad utilizzare sistemi di file sharing tramite computer di proprietà della scuola.
- divieto di aggirare le regole di sicurezza imposte sugli strumenti informatici e sulle reti di collegamento interne;
- divieto di aggirare gli strumenti informatici di filtro/monitoraggio;
- divieto di alterare e/o modificare documenti informatici aventi efficacia probatoria;
- il divieto della connessione, consultazione, navigazione, streaming ed estrazione mediante downloading, a siti web che siano considerabili illeciti (e quindi, a titolo esemplificativo, giocare in borsa, siti pornografici, siti che presentino contenuti contrari alla morale, alla libertà di culto ed all'ordine pubblico, che consentano la violazione della privacy, che promuovano e/o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica, ovvero che violino le norme in materia di copyright e di proprietà intellettuale).

Qualunque violazione delle modalità sopra indicate viene perseguita, civilmente e penalmente.

Attività consentite (policy) al supervisore di sistema o a un suo delegato:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 5;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete dell'ITA "G. GARIBALDI" tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e, limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore del sistema informatico e/o l'amministratore del dominio possono regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore del sistema informatico può adottare appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad un dispositivo cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password.

Sanzioni
In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia.
Chiunque (personale Docente, Educativo, A.T.A. e Alluni) utilizzi internet non rispettando la POLICY, incorrerà in sanzioni disciplinari.

Gestione di strumenti informatici

Per i server che ospitano i database sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia; tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup sono realizzate su unità BACKUP-NAS;
- divieto di utilizzare floppy disk e/o pen drive come mezzo per il backup; divieto per gli utilizzatori di computer di lasciare incustodito, o accessibile, il computer stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screen saver automatico dopo 2 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta; divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati; divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem elinee telefoniche.
- divieto di utilizzare sistemi di P2P (winmx, kazaa, emule, ecc….); utilizzare social network (face book, messanger, net log, ecc…)

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.
Il fax si trova nell'ufficio del Direttore S.G.A. e l'utilizzo è consentito unicamente agli incaricati del trattamento dei dati.
La manutenzione dei computer, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

Controlli previsti e sanzioni

Utilizzo del registro elettronico da parte dei docenti

Al personale docente sono rilasciate apposite credenziali identificative (login e password) per accedere all'applicativo del registro elettronico. Il personale docente è tenuto ad osservare la politica di gestione delle credenziali, inserita nel Documento Programmatico sulla Sicurezza.

Nel rispetto della normativa vigente richiamata nelle premesse del presente disciplinare, l'istituzione scolastica non procede a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori. L'Amministrazione, in persona del Dirigente Scolastico, si riserva la facoltà di eseguire controlli in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare, dalla normativa posta a protezione dei dati personali.
I controlli sono posti in essere dal Titolare del trattamento dati coadiuvato dall'amministratore di sistema. I controlli sono eseguiti tenendo conto del principio di graduazione (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati

Personali 1/3/2007) al verificarsi di comportamenti anomali, il dirigente deve effettuare un controllo anonimo su dati aggregati, riferito all'intera struttura amministrativa oppure a sue aree. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo degli strumenti dell'amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite ai dipendenti in assenza di successive anomalie non si effettueranno controlli su base individuale:

- in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli
- in caso di riscontrato e reiterato uso non conforme delle risorse informatiche, verrà attivato il procedimento disciplinare nelle forme e con le modalità di cui al D.lgs. n. 165 del 2001 articoli 55 bis e seguenti.

::

Fonti di documentazione

Il Documento Programmatico sulla Sicurezza è stato predisposto consultando le seguenti fonti:

http://www.garanteprivacy.it

http://www.osservatoriotecnologico.net

D.M. n. 305 del 7.12.2006, Regolamento concernente l'"identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal MPI, in attuazione dell'art. 20 e 21 decreto del

legislativo 30.6.2003 n. 96 (il «Codice in materia di protezione dei dati personali»)"*;*

Codice dell'amministrazione digitale;

Direttiva n. 02/09 del 26/05/2009 Dipartimento della Funzione Pubblica;

Anagrafe degli studenti (DLgs 76/2005 e Ordinanze Ministeriali varie);

Garante Privacy: "La privacy tra i banchi di scuola"

Garante Privacy comunicato stampa del 10/12/2009; Decreto legge 5/2012 convertito in Legge 35/2012

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Il Direttore S.G.A.	Il Dirigente Scolastico
Responsabile del trattamento dei dati	Titolare del trattamento dei dati
DSGA: Pietro Lauri	Prof.ssa Patrizia Marini

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005
Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007
E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Aggiornamento del 22 marzo 2018:

Il Consiglio dei Ministri, nella seduta n. 75 del 21 marzo 2018, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Indice degli allegati

Allegato n. 1: Informativa per il trattamento dei dati personali degli alunni e delle loro famiglie

Allegato n. 2: Informativa al personale art. 13 D.Lgs. n.196/2003 per il trattamento dei dati personali del personale dipendente.

Allegato n. 3: Informativa a fornitori, enti e associazioni art. 13 D.Lgs. n.196/2003 per il trattamento dei dati delle aziende fornitrici o degli enti e associazioni che hanno rapporti con la scuola

Allegato n 4: Richiesta di comunicazione e diffusione di dati sugli esiti scolastici nell'interesse dell'alunno ex art. 96 D.L.vo 196/03

Allegato n 5: Procedura per l'utente di comunicazione al custode delle password l'avvenuta modifica della password

REGIONE LAZIO

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005

Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007

E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Allegato 1: Informativa per il trattamento dei dati personali degli alunni e delle loro famiglie

Gentile Signore/a,

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), questa Istituzione scolastica per espletare le sue funzioni istituzionali e, in particolare, per gestire le attività di istruzione, educative e formative stabilite dal Piano dell'Offerta Formativa Triennale, deve acquisire dati personali che Vi riguardano, inclusi quei dati che il D.lgs 196/2003 definisce "dati sensibili e giudiziari".

Ai sensi del decreto del Ministero della Pubblica Istruzione n.305 del 7 dicembre 2006 che ha individuato i dati sensibili e giudiziari che le amministrazioni scolastiche sono autorizzate a tutelare, indicando anche le operazioni ordinarie che i diversi titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge, Vi informiamo che, per le esigenze di gestione sopra indicate, possono essere oggetto di trattamento le seguenti categorie di dati sensibili e giudiziari:

1. i dati personali da Lei forniti, che riguardano l'alunno che usufruirà dei nostri servizi o i suoi familiari, verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, così come definite dalla normativa vigente (R. D. n. 653/1925, D. Lgs. n. 297/1994, D.P.R. n. 275/1999, Legge n. 104/1992 Legge n. 53/2003 e normativa collegata);

2. i dati personali definiti come "dati sensibili" o come "dati giudiziari" dal suddetto codice, che Lei ci fornisce in questo momento e quelli che ci fornirà successivamente, saranno trattati dalla scuola secondo quanto previsto dalle disposizioni di legge, in considerazione delle finalità di rilevante interesse pubblico che la scuola persegue, con le modalità previste dal regolamento adottato con decreto 7 dicembre 2006, n. 305. I dati sensibili sono, ai sensi dell'art. 4 del Codice, lettera d, quei dati personali "*idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"*. I dati giudiziari sono quei dati personali idonei a rivelare procedimenti o provvedimenti di natura giudiziaria;
3. il conferimento dei dati richiesti è obbligatorio poiché necessario alla realizzazione delle finalità istituzionali richiamate al punto 1; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti servizi necessari per garantire il suo diritto all'istruzione ed alla formazione;
4. il trattamento sarà effettuato sia con modalità manuali sia mediante l'uso di procedure informatiche;
5. i dati sensibili e giudiziari saranno oggetto di comunicazione ad altri soggetti pubblici e privati nella misura strettamente indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni in materia sanitaria o giudiziaria, secondo le disposizioni del regolamento adottato con decreto 7 dicembre 2006, n. 305;
6. i dati personali diversi da quelli sensibili e giudiziari potranno essere comunicati esclusivamente a soggetti pubblici se previsto da disposizioni di legge o regolamento; in caso contrario potranno essere trattati attivando la procedura prevista dall'art. 39 del Codice; i dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola secondo le vigenti disposizioni in materia;
7. ai sensi dell'art. 96 del Codice, ferma restando la tutela della riservatezza dell'alunno di cui all'articolo 2, comma 2, del D.P.R. 24 giugno 1998, n. 249, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, dell'alunno per il quale si richiede l'iscrizione, i dati relativi agli esiti scolastici, intermedi e finali, ed altri dati personali diversi da quelli sensibili o giudiziari potranno essere comunicati o

diffusi, anche a privati e per via telematica. La comunicazione avverrà esclusivamente a seguito di Sua richiesta e i dati saranno poi trattati esclusivamente per le predette finalità;

Sono adottate dalla scuola le misure minime per la sicurezza dei dati personali previste

I dati oggetto di trattamento potranno essere comunicati ai seguenti soggetti esterni all'istituzione scolastica per le seguenti finalità:

- Al Miur e all'USR-Regione Lazio per l'anagrafe studenti
- Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
- Agli Enti Locali per la fornitura dei servizi ai sensi del D.lg. 31 marzo 1998, n.112, limitatamente ai dati indispensabili all'erogazione del servizio;
- Agli Istituti di assicurazione per denuncia infortuni e per la connessa responsabilità civile;
- All'INAIL per la denuncia infortuni ex D.P.R. 30 giugno 1965, n.1124
- Alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104
- Alle AUSL in riferimento agli obblighi connessi alla L. 119/2017 e al trattamento dei dati vaccinali
- Alle aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e D.lgs 21 aprile 2005, n. 77 e, facoltativamente per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
- Alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- Alle Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;

Vi ricordiamo infine:

- che, ai sensi dell'art.24 del D.lgs 196/2003, in alcuni casi il trattamento può essere effettuato anche senza il consenso dell'interessato;
- che in ogni momento potrete esercitare i Vostri diritti nei confronti del titolare del trattamento.

- Il titolare del trattamento è la Prof.ssa Patrizia Marini in qualità di Dirigente Scolastico e dunque legale rappresentante pro-tempore dell'Istituto Tecnico Agrario Statale "G. GARIBALDI" - Via Ardeatina 524-00178 Roma tel. 06.121127241;
- Il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi è il DSGA Pietro Lauri
- Gli incaricati al trattamento dati sono gli assistenti amministrativi espressamente autorizzati all'assolvimento di tali compiti e i docenti identificati ai sensi di legge, ed edotti dei vincoli imposti dal D.lgs.

Il Dirigente Scolastico
Prof.ssa Patrizia Marini

ROMA, lì *Firma dei Genitori*

Ministero dell'Istruzione, dell'Università e della Ricerca - Ufficio Scolastico Regionale per il Lazio
ISTITUTO TECNICO AGRARIO "GIUSEPPE GARIBALDI"

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005
Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007
E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Allegato 2: Informativa al personale art. 13 D.Lgs. n.196/2003 per il trattamento dei dati personali del personale dipendente.

Gentile Signore/a,
secondo le disposizioni del Decreto Legislativo 30 giugno 2003, n.196 *("Codice in materia di protezione dei dati personali")* nel seguito indicato sinteticamente come *Codice*, il trattamento dei dati personali che La riguardano sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.
Ai sensi dell'articolo 13 del *Codice*, Le forniamo, quindi, le seguenti informazioni:
1. i dati personali da Lei forniti verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, incluse le finalità di instaurazione e gestione dei rapporti di lavoro di qualunque tipo, così come definite dalla normativa vigente (R.D. n. 653/1925, D. Lgs. n. 297/1994, D.P.R. n. 275/1999, Legge n. 104/1992, Legge n. 53/2003, D. Lgs, n. 165/2001, D. lgs. n. 151/2001, l'art. 112 del *Codice*, i Contratti Collettivi di Lavoro Nazionali ed Integrativi stipulati ai sensi delle norme vigenti, la normativa collegata alle citate disposizioni);
2. i dati personali definiti come "dati sensibili" o come "dati giudiziari" dal suddetto codice, che Lei ci ha fornito e quelli che ci fornirà in occasioni successive, saranno trattati dalla scuola secondo quanto previsto dalle disposizioni di legge e di regolamento citate al precedente punto 1 ed in considerazione delle finalità di rilevante interesse pubblico che la scuola persegue e delle finalità di interesse pubblico costituite dalla gestione dei rapporti di lavoro di qualunque tipo, come stabilito dall'art. 112 del *Codice*. Le ricordiamo che i dati sensibili sono quei dati personali *"idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"*. I dati giudiziari sono quei dati personali idonei a rivelare procedimenti o provvedimenti di natura giudiziaria;
3. il conferimento dei dati richiesti è obbligatorio in quanto previsto dalla normativa citata al precedente punto 1; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento o mantenimento del rapporto di lavoro;
4. il trattamento sarà effettuato sia con modalità manuali che mediante l'uso di procedure informatiche;
5. i dati sensibili e giudiziari non saranno oggetto di diffusione; tuttavia alcuni di essi potranno essere comunicati ad altri soggetti pubblici nella misura strettamente indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni in materia di rapporto di lavoro pubblico, sanitaria o giudiziaria;
6. i dati personali diversi da quelli sensibili e giudiziari potranno essere comunicati esclusivamente a soggetti pubblici secondo quanto previsto dalle disposizioni di legge e di regolamento di cui al precedente punto 1;
7. il titolare del trattamento è la **Prof.ssa Marini** in qualità di Dirigente Scolastico e dunque legale rappresentante pro-tempore dell'Istituto Tecnico Agrario Statale "G. GARIBALDI" - Via Ardeatina 524-00178 Roma tel. 06.121127241
8. il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi è il **DSGA Lauri Pietro**
9. al titolare del trattamento o al responsabile Lei potrà rivolgersi senza particolari formalità, per far valere i Suoi diritti, così come previsto dall'articolo 7 del Codice, che per Sua comodità riproduciamo integralmente:

Art. 7 (Diritto di accesso ai dati personali ed altri diritti)
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venire a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, "integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il Dirigente Scolastico
Prof.ssa Patrizia Marini

Ministero dell'Istruzione, dell'Università e della Ricerca - Ufficio Scolastico Regionale per il Lazio
ISTITUTO TECNICO AGRARIO "GIUSEPPE GARIBALDI"

REGIONE LAZIO

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005
Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007
E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Allegato 3: Informativa a fornitori, enti e associazioni art. 13 D.Lgs. n.196/2003 per il trattamento dei dati delle aziende fornitrici o degli enti e associazioni che hanno rapporti con la scuola

Spett. …….....
Via…….
…….

secondo le disposizioni del Decreto Legislativo 30 giugno 2003, n.196 *("Codice in materia di protezione dei dati personali")* nel seguito indicato sinteticamente come *Codice*, il trattamento dei dati che Vi riguardano sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Vs. riservatezza e dei Vs. diritti.

Ai sensi dell'articolo 13 del *Codice*, Vi forniamo, quindi, le seguenti informazioni:

1. i dati da Voi forniti verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, incluse le finalità di instaurazione e gestione dei rapporti di lavoro di qualunque tipo, e quelle relative alla conclusione di contratti di fornitura di beni e/o servizi, così come definite dalla normativa vigente (R.D. n. 653/1925, D. Lgs. n. 297/1994, D.P.R. n. 275/1999, Decreto Interministeriale 1 febbraio 2001, n. 44, norme in materia di contabilità generale dello Stato e normativa collegata);

2. il conferimento dei dati richiesti è obbligatorio in quanto previsto dalla normativa citata al precedente punto 1; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento o mantenimento dei contratti di fornitura di beni e servizi;

3. il trattamento sarà effettuato sia con modalità manuali che mediante l'uso di procedure informatiche;

4. i dati potranno essere comunicati esclusivamente a soggetti pubblici secondo quanto previsto dalle disposizioni di legge e di regolamento di cui al precedente punto 1;

5. il titolare del trattamento è la **Prof.ssa Marini** Patrizia in qualità di Dirigente Scolastico e dunque legale rappresentante pro-tempore dell'Istituto Tecnico Agrario Statale "G. GARIBALDI" - Via Ardeatina 524-00178 Roma tel. 06.121127241*;*

6. il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi: **DSGA Lauri Pietro**

7. al titolare del trattamento o al responsabile Vi potrete rivolgere senza particolari formalità, per far valere i Vs. diritti, così come previsto dall'articolo 7 del Codice, che per Vs. comodità riproduciamo integralmente:

Art. 7 (Diritto di accesso ai dati personali ed altri diritti)

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venire a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, "integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il Consiglio dei Ministri, nella seduta n. 75 del 21 marzo 2018, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Dirigente Scolastico
Prof.ssa Patrizia Marini

Ministero dell'Istruzione, dell'Università e della Ricerca - Ufficio Scolastico Regionale per il Lazio
ISTITUTO TECNICO AGRARIO "GIUSEPPE GARIBALDI"

REGIONE LAZIO

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005
Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007
E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Allegato n 4: Richiesta di comunicazione e diffusione di dati sugli esiti scolastici nell'interesse dell'alunno ex art. 96 D.L.vo 196/03

Al Dirigente Scolastico
ISTITUTO TECNICO AGRARIO
"Giuseppe GARIBALDI"
Via Ardeatina, 524
00178, Roma

Oggetto: **Richiesta di comunicazione e diffusione di dati sugli esiti scolastici nell'interesse dell'alunno ex art. 96 D.L.vo 196/03**

Il sottoscritto _____ Alunno della classe quinta Sez… di questo ISTITUTO TECNICO AGRARIO:

- avendo conseguito il diploma conclusivo del corso di studi frequentato nel corrente anno scolastico presso l'Istituto;
- ricevuta l'informativa di cui all'art 13 D.L.vo 196/2003

Visto l'art. 96 del D.Lgs. n. 196/2003, qui riportato testualmente:

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13;
2. I dati possono essere successivamente trattati esclusivamente per le predette finalità;
3. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati"**;**

chiede, Accetta e Autorizza

che sia applicata nei suoi confronti, fino ad una eventuale successiva diversa disposizione e/o revoca, la possibilità, prevista al comma 1 di tale articolo, di comunicare o diffondere, anche a privati e per via telematica, dati relativi ai propri esiti scolastici, intermedi e finali, e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle finalità previste da tale disposizione normativa (nome, cognome, luogo e data di nascita, indirizzo, numero di telefono, fax, e-mail, nonché il possesso di titoli ed eventuali specializzazioni).
Dichiara che la presente funge anche da informativa per tali dati e finalità.

Luogo e data

(Nome Cognome)

_____
(firma leggibile)

Ministero dell'Istruzione, dell'Università e della Ricerca - Ufficio Scolastico Regionale per il Lazio
ISTITUTO TECNICO AGRARIO "GIUSEPPE GARIBALDI"

1872 2017

VIA ARDEATINA, 524 – 00178 ROMA - XIX Distretto – RMTA070005
Tel. 06/121127240 - Fax 06/5033124 - Cod. Fisc.: 80185390582 – P.IVA Azienda: 02132081007
E-mail: rmta070005@istruzione.it - PEC:rmta070005@pec.istruzione.it - Sito web www.itasgaribaldi-roma.gov.it

Allegato 5: Comunicazione al custode delle password dell'avvenuta modifica della password da parte degli incaricati del trattamento di dati personali con elaboratori elettronici

Conformemente a quanto previsto Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), l'"incaricato della custodia delle parole chiave" necessarie per accedere agli elaboratori elettronici in uso presso gli uffici dell'Istituzione scolastica Istituto Tecnico Agrario Statale "Giuseppe Garibaldi" in Via Ardeatina 524 Roma, dovrà usare la massima riservatezza e discrezione nella gestione delle parole chiave e nella loro protezione, anche con riferimento agli obblighi che ne derivano dalla qualifica professionale. In particolare, l'incaricato della custodia delle parole chiave dovrà:

- ricevere dagli incaricati del trattamento di dati personali con elaboratori elettronici la busta chiusa contenente la nuova parola chiave da essi elaborata e che essi hanno provveduto a sostituire autonomamente con la prevista periodicità;
- custodire le parole chiave attribuite dagli incaricati del trattamento di dati personali con elaboratori elettronici;
- nel caso in cui il titolare del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza abitualmente (per malattia, ferie, etc.), consegnare al titolare stesso la busta contenente la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo (ad es., effettuazione di interventi di riparazione, assistenza, aggiornamento antivirus, etc.);
- informare tempestivamente l'incaricato del quale, in sua assenza, è stata consegnata la parola chiave al titolare del trattamento, affinché questi provveda immediatamente alla sostituzione della parola chiave e la consegni al custode in una nuova busta chiusa.