



ISTITUTO COMPRENSIVO STATALE "ALDA COSTA"

Scuola dell'infanzia "G. B. Guarini" – Scuole primarie "A. Costa" – "G. B. Guarini" – "A. Manzoni"
Scuola Secondaria di I grado "M. M. Boiardo" - "Sezione Ospedaliera"
Sede: Via Previati, 31 – 44121 Ferrara Tel. 0532/205756 – Fax 0532/241229
e-mail feic810004@istruzione.it PEC feic810004@pec.istruzione.it - <http://scuole.comune.fe.it/>
C.F. 93076210389 - COD. MEC. FEIC810004

FUTURA

LA SCUOLA PER L'ITALIA DI DOMANI



Prot. vedesi segnatura

FERRARA, 2/10/2024

Oggetto

Regolamento UE 2016/679 e D.Lgs. n. 196/2003 (come modificato dal D. lgs n. 101 del 10 agosto 2018, contenente Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679) – Incarico di Amministratore di Sistema

La sottoscritta Allegretta Antonietta, Dirigente Scolastico e rappresentante legale dell'Istituto, titolare del trattamento dei dati ai sensi del Regolamento U.E. 679/2016 e del D.lgs n. 196 del 30/6/2003 (come modificato dal D. lgs n. 101 del 10 agosto 2018, contenente Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679),

- VISTO il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;
- VISTO L'art. 4, comma 1, punto 1) del Regolamento UE 2016/679 che definisce quale «dato personale» qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); e considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- VISTO L'art. 9, comma 1, del Regolamento UE 2016/679 definisce specifiche categorie di dati personali particolari, quali quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici

intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

VISTO L'art. 10 del Regolamento UE 2016/679 che prevede le modalità di trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

VISTA la circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni» con l'obiettivo di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi;

VISTI gli allegati 1 e 2 alla circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale;

VISTO l'art. 32 del Regolamento UE 2016/679, recante norme sulla sicurezza del trattamento dei dati; 

VISTO il Codice dell'Amministrazione Digitale (CAD) di cui al D.lgs. 82/2005, come modificato dal D.lgs. 179/2016, attuativo dell'art. 1 della Legge 124/2014 di riforma della Pubblica Amministrazione (cd. Legge Madia);

VISTO il "Provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008;

CONSIDERATE le capacità e l'affidabilità nonché l'esperienza richieste nel campo dei sistemi informativi al fine dell'espletamento dell'incarico;

CONSIDERATO che l'incarico in oggetto attiene a fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati e alla sicurezza informatica;

nomina

Il Signor Marco Verri con l'accettazione di tale incarico ,Amministratore di Sistema,di questa Istituzione Scolastica.

Il Signor Marco Verri si impegna ad operare personalmente nonché a dare direttive al personale, in relazione a:

- a) sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare la coerenza con gli standard tecnici e organizzativi comuni;
- b) sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del Codice dell'Amministrazione Digitale (CAD);
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità

anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

- e) report di analisi periodica della coerenza tra l'organizzazione della amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione;
- f) cooperazione alla revisione della riorganizzazione della amministrazione ai fini di cui alla lettera e);
- g) pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) esecuzione delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni;
- j) adeguamento delle operazioni di trattamento dei dati agli standard di sicurezza, al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta

In particolare, l'Amministratore di Sistema dovrà:

- impostare e gestire, in collaborazione con le altre figure preposte, un sistema di autenticazione informatica per i trattamenti dati personali effettuati con strumenti elettronici;
- adottare un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici (autenticazione informatica) da parte degli Amministratori e degli utenti per le postazioni contenenti dati particolari; le registrazioni (access log) devono avere caratteristiche adeguate agli standard di sicurezza;
- disattivare i codici identificativi in caso di mancato utilizzo per un periodo superiore a sei mesi;
- assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall) adeguati agli standard di sicurezza;
- distruggere i supporti di memorizzazione nel caso in cui non siano più riutilizzati;
- organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica di eventuali tentativi di accessi non autorizzati al sistema proveniente da soggetti terzi;
- monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al Titolare del Trattamento tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e quantità dei dati personali trattati;
- predisporre in collaborazione con il Titolare del Trattamento un piano di controlli periodici, adeguati agli standard di sicurezza;

- gestire le password di Amministratore di Sistema e di utenti con privilegi;

conformarsi alle procedure indicate nel Codice dell'Amministrazione Digitale (CAD) in relazione al mancato rispetto delle norme di sicurezza e in caso di eventuali incidenti

Il soggetto incaricato, accettando l'incarico, dichiara di essere a conoscenza e di rispettare quanto stabilito dal Regolamento UE 2016/679 e dal D.lgs. n. 196 del 30/06/2003 come modificato dal D. Lgs n. 101 del 10 agosto 2018, e in particolare:

1. di garantire un sistema di sicurezza idoneo a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
2. di attenersi agli obblighi di assoluta riservatezza connessi al suo incarico;
3. di trattare dati personali solo per quanto indispensabile in relazione all'assolvimento degli incarichi assegnati;
4. di vigilare affinché il trattamento dei dati da parte del personale posto alle dirette dipendenze o delle società controllate e/o partecipate avvenga in modo lecito e secondo correttezza;
5. di impartire istruzioni ad eventuali incaricati, vigilandone l'operato affinché siano garantite le misure minime di sicurezza di cui sopra;
6. di interagire con l'Autorità Garante, in caso di richieste o di informazioni o effettuazione di controlli o di accessi da parte dell'autorità;
7. di rispettare le prescrizioni impartite dal titolare, tra cui il divieto assoluto di comunicare e diffondere a terzi non autorizzati le informazioni e i dati personali di cui sia venuto a conoscenza e l'impegno ad informare prontamente il titolare in caso di mancato rispetto delle norme di sicurezza e in caso di eventuali incidenti o più in generale di ogni questione rilevante ai fini della legge.
8. di conoscere, rispettare ed essere sempre conforme al Regolamento UE 2016/679, con particolare ma non esclusivo riguardo agli artt. da 24 a 39, impegnandosi a collaborare con il Titolare del Trattamento per il rispetto delle prescrizioni ivi contenute.

L'operato dell'Amministratore di Sistema sarà oggetto, con cadenza annuale ad un'attività di verifica tesa a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti e alle procedure di sicurezza informatica previste dal Codice dell'Amministrazione Digitale (CAD).

L'Amministratore di Sistema dichiara di accettare l'incarico sopra conferito .

Il Dirigente Scolastico

D.ssa Antonietta Allegretta