Ministero dell'Istruzione – Ufficio Scolastico Regionale per il Lazio

Istituto Comprensivo Castelverde

www.iccastelverderoma.edu.it

Via Massa di San Giuliano, 131 – 00132 ROMA Tel. 06 455 90 500
PEO: rmic8cp00e@istruzione.it - PEC: rmic8cp00e@pec.istruzione.it
Codice meccanografico: RMIC8CP00E Codice fiscale: 97616500589
IPA - Codice univoco ufficio per Fatturazione Elettronica: UFEHD1

Il/La sottoscritto/a ……

nato/a ……. Prov. …….. il ……..…

residente a …….. Via ……..……..

Cap. ……. Tel. ……..…… Cell. ……...……..

domicilio a ……..…….. Via ……..……...

Cap. ……. Tel. ……..…… Cell. ……...…

Codice fiscale ….!.....!....!.....!.....!.....!.....!.....!.....!.....!.....!.....!.....!.....!.....

Email …….....

NUMERO DI PARTITA DI SPESA FISSA ……..……

- ASSISTENTE AMMINISTRATIVO a TEMPO INDERTERMINATO / DETERMINATO
- COLLABORATORE SCOLASTICO a TEMPO INDERTERMINATO / DETERMINATO
- DOCENTE INFANZIA a TEMPO INDERTERMINATO / DETERMINATO
- DOCENTE PRIMARIA a TEMPO INDERTERMINATO / DETERMINATO
- DOCENTE SCUOLA SECONDARIA DI I GRADO classe di concorso ……...……

Per n° ore ..... A TEMPO INDERTERMINATO / DETERMINATO

Istituto di completamento…… n° ore …….

Scuola di provenienza ……dal ……...…al……...…….

ASL di appartenenza ……...… Via ……...……..n. ……

DICHIARA

Di assumere servizio in data odierna

Roma, ……..

Firma

……

MOD. C (INFORMAZIONI CONTABILI)

Cognome……..…..Nome……..…….

Il/La sottoscritto/a a conoscenza delle sanzioni previste dal codice penale e dalle altre disposizioni di legge in materia, in caso di dichiarazioni mendaci, dichiara sotto la sua personale responsabilità:

- **C/C GIA' PRESENTE AL SISTEMA**

- **ACCREDITAMENTO SUL CONTO CORRENTE BANCARIO**

IBAN ……..……

ABI ……

CAB ……...

CIN ……....

C/C Nr ……..……..……

- **ACCREDITAMENTO SUL CONTO CORRENTE POSTALE**

IBAN ……..

ABI …….

CAB ……

CIN …….

C/C Nr ……

Roma …… Firma

……

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONI
(At. 46 D.P.R. 445 del 28/12/2000)

Il/La sottoscritto/a _____
(cognome) (nome)

Noto/a a _____(_____) il _____
(comune di nascita ; se nato/a all'estero specificare lo stato) (prov.)

residente _____ (_____)
(comune di residenza) (prov.)

in Via/Piazza /Largo _____n. _____

consapevole delle sanzioni penali, nel caso di dichiarazoni non veritiere e falsità negli atti, richiamate dall'art. 76 D.P.R. 445 del 28/12/2000

DICHIARA

- o Di essere nato/a _____(_____) il _____
  (comune di nascita ; se nato/a all'esterospecificare lo stato) (prov.)
- o Di essere cittadino italiano oppure _____
- o Di godere dei diritti civili e politici
- o Di possedere il seguente titolo di studio _____

  rilasciato dalla scuola / università di _____
- o Di aver conseguito l'abilitazione all'insegnamento per _____

  mediante _____
- o Di non aver riportato condanne penali e di non essere destinatario di provvedimenti che riguardano l'applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi iscritti nel casellario giuziale ai sensi della vigente normativa
- o Di non essere a conoscenza di essere sottoposto a procedimenti penali

Barrare la/e voci che riguardano la/e dichiarazione/i da produrre.

Luogo e data Il/La dichiarante

_____ _____

La presente dichiarazione non necessita dell'autenticazione della firma e sostituisce a tutti gli effetti le normali certificazioni richieste o destinate ad una pubblica amministrazione nonché ai gestori di pubblici servixi e ai privati che vi consentono.
Informativa ai sensi dell'art. 13 del Decreto legislativo n. 196/03: i dati sopra riportati sono prescritti dalle disposizioni vigenti ai finidel procedimento per il quale sono richiesti e verranno utilizzati esclusivamente per tale scopo.

Ministero dell'Istruzione – Ufficio Scolastico Regionale per il Lazio

Istituto Comprensivo Castelverde

www.iccastelverderoma.edu.it

Via Massa di San Giuliano, 131 – 00132 ROMA Tel. 06 455 90 500
PEO: rmic8cp00e@istruzione.it - PEC: rmic8cp00e@pec.istruzione.it
Codice meccanografico: RMIC8CP00E Codice fiscale: 97616500589
IPA - Codice univoco ufficio per Fatturazione Elettronica: UFEHD1

Alle unità organizzative:
"Personale docente interno ed esterno
"Collaboratori del Dirigente scolastico/Staff di direzione"
All'albo dell'Istituto SEDE

INFORMATIVA
per il trattamento dei dati personali del personale docente interno ed esterno e Collaboratori DS
(ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679)

Introduzione
Il Regolamento generale (UE) 2016/679 sulla protezione dei dati (d'ora in poi Regolamento) prescrive l'osservanza di regole a protezione di tutti i dati personali, nelle fasi del loro trattamento, della loro diffusione, conservazione e distruzione durante l'attività amministrativa e istituzionale. In ottemperanza a tale normativa si informa che il trattamento di tutti i dati personali sarà improntato ai principi di correttezza, liceità, trasparenza e tutela della riservatezza dei diritti del personale docente interno ed esterno.

Titolare del trattamento e responsabile della protezione dei dati (RPD)
Titolare del trattamento: Istituto Comprensivo CASTELVERDE, con sede legale in via Massa San Giuliano, 131 - 00132 Roma, in persona del legale rappresentante Dirigente Scolastico Nicola Armignacca, PEC: rmic8cp00e@pec.istruzione.it.

Responsabile della protezione dei dati: ai sensi dell'art. 37, comma 1 del Regolamento, è stato designato il Responsabile della Protezione dei Dati (RPD), figura deputata ad assolvere funzioni di supporto e controllo, consultive, formative ed informative in relazione all'applicazione del Regolamento; di seguito il nominativo e l'indirizzo di contatto: Ing. Marco MAGAZZENI, e-mail: info@rlsicurezza.it – PEC: mmgformazione@legalmail.it.

Finalità e base giuridica del trattamento
Nel corso del rapporto i dati personali e le particolari categorie di dati previste dagli art. 9 e 10 del Regolamento, saranno trattati esclusivamente dal personale di questo istituto appositamente incaricato, secondo quanto previsto dal Regolamento, dalle disposizioni di legge e di regolamento statali e regionali in materia, nel rispetto del principio di stretta indispensabilità dei trattamenti (privacy by default).
Il conferimento dei dati può essere obbligatorio o facoltativo. È da considerarsi obbligatorio il conferimento dei dati necessario alla realizzazione delle finalità istituzionali di interesse pubblico dell'istituzione scolastica. L'eventuale diniego al trattamento di tali dati potrebbe determinare il mancato perfezionamento del rapporto di lavoro o comportare la mancata instaurazione o continuazione dello stesso.

A tal fine sono da considerarsi strettamente necessari all'esercizio delle funzioni istituzionali, i dati personali necessari per la gestione:

- di tutte le fasi del rapporto di lavoro: assunzione, adempimenti retributivi, contributivi, assicurativi, fiscali, contrattuali e legali;
- dell'organizzazione dell'attività didattica e delle altre attività istituzionali dell'istituto.

L'istituzione scolastica potrà trovarsi nella necessità di trattare, per finalità istituzionali di rilevante interesse pubblico, le categorie di dati personali sensibili citati nell'art. 9 comma 1 del Regolamento, che sono idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, 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 e le categorie di dati giudiziari richiamati nell'art. 10 del Regolamento quali condanne penali, reati o connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1 del Regolamento.
Le finalità del trattamento dei dati sensibili e giudiziari, ai sensi dell'art. 6, comma 1, lettera e) del Regolamento, così come sancito dal Decreto ministeriale 7 dicembre 2006 n. 305, sono da intendersi:

1. in riferimento alla selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro, nei quali vengono trattati:
   a) i dati inerenti lo stato di salute per l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;
   b) i dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
   c) i dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;
   d) i dati sulle convinzioni filosofiche o d'altro genere che possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;
   e) i dati di carattere giudiziario che sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato;
   f) le informazioni sulla vita sessuale che possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.
2. in riferimento alla gestione del contenzioso e procedimenti disciplinari, nella quale vengono trattati dati sensibili e giudiziari concernenti tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e della istituzione scolastica nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.
3. In riferimento agli Organismi collegiali e commissioni istituzionali, nei quali il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentati delle organizzazioni sindacali.

L'acquisizione e il trattamento di questa tipologia di dati verrà trattata nel rispetto del principio di indispensabilità del trattamento (privacy by default) e avverrà soltanto secondo quanto previsto dalle disposizioni di legge ed in considerazione delle finalità di rilevante interesse pubblico che l'istituzione scolastica persegue o se indicati nelle Autorizzazioni Generali del Garante per la protezione dei dati. Di norma non saranno soggetti a diffusione, salvo la necessità di comunicare gli stessi ad altri Enti Pubblici nell'esecuzione di attività istituzionali previste da norme di legge in ambito sanitario, previdenziale, tributario, infortunistico, giudiziario.

Per taluni procedimenti amministrativi attivabili soltanto su domanda individuale dell'interessato (ottenimento di particolari servizi, prestazioni, benefici, esenzioni, certificazioni, ecc.) può essere indispensabile, per il raggiungimento della finalità richiesta, il conferimento di ulteriori dati (dati personali facoltativi). In tali casi verrà fornita un'integrazione scritta alla presente informativa.

Modalità di trattamento dei dati

I dati personali del personale docente vengono acquisiti direttamente presso l'interessato (art. 13 del Regolamento) e/o ottenuti presso terzi, ad esempio dalla scuola di provenienza nei casi di trasferimento (art. 14 del Regolamento).

Il trattamento prevede le fasi di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, raffronto o interconnessione, limitazione, cancellazione e distruzione.

A garanzia dei diritti dell'interessato, il trattamento dei dati è svolto secondo le modalità e le cautele previste dal Regolamento, rispettando i presupposti di legittimità di ciascuna richiesta, seguendo principi di correttezza, trasparenza, tutela della dignità e riservatezza dell'interessato.

Il trattamento verrà svolto in forma cartacea e/o attraverso strumenti informatici e telematici; i relativi dati saranno conservati negli archivi presenti presso questo istituto, negli archivi del MIUR[1] e suoi organi periferici (Ufficio Scolastico Regionale, Ambito Territoriale Provinciale, ecc.).

I dati su strumenti informatici e telematici verranno trattati e conservati secondo le regole tecniche di conservazione digitale indicate dall'AGID[2]. I dati cartacei, invece, saranno conservati secondo i piani di conservazione e scarto indicati dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali.

Destinatari dei dati personali

I soggetti che tratteranno i dati personali dell'interessato nell'ambito delle attività istituzionali di questo istituto sono riportati nella tabella seguente:

UNITÀ ORGANIZZATIVA	TRATTAMENTI ASSOCIATI	TRATTAMENTI CHE UTILIZZANO DATI SENSIBILI E GIUDIZIARI
Dirigente Scolastico (Titolare del Trattamento)	**T3** - Personale dipendente - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 1**: selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro
	T4 - Collaborazioni professionali - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 2**: gestione del contenzioso e procedimenti disciplinari
	T7 - Gestione istituzionale e Protocollo - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 3**: organismi collegiali e commissioni istituzionali
	T8 - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali	
	T9 - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario	
Collaboratori del dirigente scolastico /	**T3** - Personale dipendente - Dati personali trattati da Assistenti	**Scheda n. 1**: selezione e reclutamento a tempo

[1] Ministero dell'Istruzione, dell'Università e della Ricerca

[2] Agenzia per l'Italia digitale

staff di direzione	amministrativi e DSGA	indeterminato e determinato, e gestione del rapporto di lavoro
	T4 - Collaborazioni professionali - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 2**: gestione del contenzioso e procedimenti disciplinari
	T7 - Gestione istituzionale e Protocollo - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 3**: organismi collegiali e commissioni istituzionali
	T8 - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali	
	T9 - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario	
Direttore dei servizi generali e amministrativi D.S.G.A. (Responsabile del trattamento)	**T3** - Personale dipendente - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 1**: selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro
	T4 - Collaborazioni professionali - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 2**: gestione del contenzioso e procedimenti disciplinari
	T7 - Gestione istituzionale e Protocollo - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 3**: organismi collegiali e commissioni istituzionali
Assistenti amministrativi	**T3** - Personale dipendente - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 1**: selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro
	T4 - Collaborazioni professionali - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 2**: gestione del contenzioso e procedimenti disciplinari
	T7 - Gestione istituzionale e Protocollo - Dati personali trattati da Assistenti amministrativi e DSGA	**Scheda n. 3**: organismi collegiali e commissioni istituzionali
Collaboratori scolastici	**T9** - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario	
Organi collegiali (Consiglio d'istituto, Giunta esecutiva, Collegio docenti, Consigli di classe)	**T8** - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali	

I dati personali, diversi da quelli indicati negli articoli 9 e 10 del Regolamento, potranno essere trattati, sempre solo ed esclusivamente per le finalità istituzionali di questo istituto, anche se raccolti presso il Ministero dell'Istruzione e le sue articolazioni periferiche, le altre Amministrazioni dello Stato, le Regioni ed Enti locali, Enti con cui questo istituto coopera in attività e progetti previsti dal Piano Triennale dell'Offerta Formativa.

I dati personali potranno essere comunicati ad altri enti pubblici o privati esclusivamente nei casi previsti dal Regolamento, specificatamente ma non esaustivamente:

1. amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;
2. servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego; organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001);
3. organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lgs. n. 81/08 e smi);
4. enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del D.P.R. n. 1124/1965;
5. amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999; organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
6. pubbliche amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
7. Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
8. organi di controllo (Corte dei Conti e MEF) al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n. 38;
9. Agenzia delle Entrate ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
10. MEF e INPDAP per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;
11. Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lgs. n. 165/2001);
12. Ministero del Lavoro e delle Politiche Sociali per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D. Lgs. 30 marzo 2001, n. 165;
13. Organi arbitrali per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
14. Avvocature dello Stato per la difesa erariale e consulenza presso gli organi di giustizia;
15. Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
16. Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza in fase giudiziale che stragiudiziale;
17. a terzi soggetti che forniscono servizi a questa istituzione scolastica quali, a titolo esemplificativo, agenzie di viaggio e strutture ricettive (esclusivamente in relazione a gite scolastiche, viaggi d'istruzione, visite didattiche), imprese di assicurazione (in relazione a polizze in materia infortunistica), eventuali ditte fornitrici di altri servizi (quali software gestionali, registro elettronico, servizi digitali, ecc.).
    La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi; in caso di trattamenti continuativi, le ditte in questione sono nominate responsabili esterni del trattamento limitatamente ai servizi resi.

La pubblicazione sul sito istituzionale e/o sul giornalino di foto di classe, riprese, foto di lavori e di attività didattiche afferenti ad attività istituzionali di questo istituto, inserite nel Piano dell'Offerta Formativa (quali ad esempio foto relative ad attività di laboratorio, visite guidate, premiazioni, partecipazioni a gare sportive, ecc.) avrà natura temporanea dal momento che le suddette immagini e video resteranno sul sito solo per il tempo necessario per le finalità cui sono destinati.

L'istituto scolastico può pubblicare sul proprio sito internet le graduatorie dei docenti per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste contengono solo i dati strettamente necessari all'individuazione del candidato, come il nome, il cognome, il punteggio e la posizione in graduatoria. Tali dati, tra l'altro, non possono rimanere pubblicati on line per un periodo superiore a quello previsto.

Trasferimento dei dati ad un paese terzo o ad un'organizzazione internazionale

I dati personali potrebbero essere comunicati, ad esempio, a seguito di trasferimento presso istituti stranieri oppure nell'ambito di viaggi di istruzione internazionali, per le finalità indicate nella presente informativa.

L'eventuale trasferimento all'estero dei dati nei paesi extra-UE avviene in conformità alle disposizioni contenute nel Capo V, articoli 45 e 46 del Regolamento.

Periodo di conservazione dei dati personali
I dati personali inerenti la carriera lavorativa del docente saranno conservati tenendo conto degli obblighi di archiviazione imposti dalla normativa vigente. Gli altri dati raccolti per l'utilizzo dei servizi e per le comunicazioni saranno conservati per i tempi stabiliti dalla normativa vigente e/o dai regolamenti interni a questo istituto.

Diritti dell'interessato
L'interessato potrà rivolgersi, in qualsiasi momento e senza particolari formalità, al Titolare del Trattamento per far valere i propri diritti, così come previsto dal Capo III del Regolamento. In sintesi l'interessato ha diritto:

- all'accesso, rettifica, cancellazione, limitazione e opposizione al trattamento dei propri dati;
- ad ottenere senza impedimenti i dati in un formato strutturato di uso comune e leggibile da dispositivo automatico per trasmetterli ad un altro titolare del trattamento (diritto alla portabilità);
- a revocare il consenso al trattamento. Tale revoca non preclude la liceità del trattamento effettuato in base al consenso prestato anteriormente alla revoca;
- a proporre reclamo al Garante per la protezione dei dati personali o altra autorità di controllo.

L'esercizio dei premessi diritti dovrà essere esercitato mediante comunicazione scritta da inviare a mezzo pec all'indirizzo rmic8cp00e@pec.istruzione.it o lettera raccomandata A/R all'indirizzo dell'Istituto Comprensivo CASTELVERDE, via Massa San Giuliano, 131 - 00132 Roma.

Processi decisionali automatizzati
Presso questo istituto non è adottato alcun processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 del Regolamento.

La presente informativa è pubblicata sul sito istituzionale, nella sezione Privacy.

Il Dirigente Scolastico
Scotto Di Carlo Diego
Firma autografa omessa ai sensi degli artt. 3, comma 2°, del d.lgs. n. 39 del 1993 e 47 del d.lgs. n. 82 del 2005

Nome: …….

Cognome: ……

Firma per presa visione

…….

Roma ……

Ministero dell'Istruzione – Ufficio Scolastico Regionale per il Lazio

Istituto Comprensivo Castelverde

www.iccastelverderoma.edu.it

Via Massa di San Giuliano, 131 – 00132 ROMA Tel. 06 455 90 500
PEO: rmic8cp00e@istruzione.it - PEC: rmic8cp00e@pec.istruzione.it
Codice meccanografico: RMIC8CP00E Codice fiscale: 97616500589
IPA - Codice univoco ufficio per Fatturazione Elettronica: UFEHD1

All'unità organizzativa "Personale docente interno ed esterno"
Al personale dell'unità organizzativa "Assistenti educativi"
All'albo dell'Istituto SEDE

DESIGNAZIONE DEGLI INCARICATI DEL TRATTAMENTO
per le unità organizzative "Personale docente interno ed esterno e Assistenti educativi"

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, d'ora in poi "Regolamento",

PREMESSO CHE titolare del trattamento è l'istituto stesso, di cui il dirigente scolastico è legale rappresentante pro-tempore;
ai sensi dell'art. 28 del Regolamento, il titolare del trattamento ha designato il DSGA quale responsabile del trattamento relativamente ai trattamenti svolti dalla funzione "Personale Amministrativo", comprendente le unità organizzative: assistenti amministrativi e collaboratori scolastici,

CONSIDERATO CHE l'art. 30 del Regolamento impone la tenuta di un registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare del trattamento;
occorre definire le misure minime di sicurezza per l'attività di ciascuna unità organizzativa nel trattamento dei dati personali;
la nomina ad incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate, bensì soltanto ricevere un'autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento;

DESIGNA

le unità organizzative "**Personale docente interno ed esterno**" e "**Assistenti educativi**" quale incaricate dei trattamenti dei dati personali elencati nell'Allegato 1.

Nell'ambito di tale designazione, il personale docente interno ed esterno e gli assistenti educativi:

1. che cessano di far parte di queste unità organizzative cessano automaticamente dalla funzione di incaricato; ogni nuovo dipendente che entra a far parte di queste unità organizzative assume automaticamente la funzione di incaricato;
2. sono autorizzati a trattare, nell'ambito dell'espletamento dell'attività di loro competenza, i dati personali con cui entrano in contatto o contenuti nelle banche dati, in archivi cartacei anche

frammentari, nelle memorie dei computer, negli archivi scolastici e dei dati personali comunque raccolti (Allegato 1 - Elenco dei trattamenti che comportano l'uso dei dati personali);

3. sono autorizzati a trattare i dati sensibili e giudiziari con cui vengono a contatto durante l'attività di loro competenza nell'ambito dell'Istituto (Allegato 1 - Elenco dei trattamenti che comportano l'uso di dati sensibili e giudiziari);
4. devono trattare i dati secondo le modalità e le finalità riportate nell'Allegato 2, comunicando gli stessi esclusivamente alle categorie di soggetti autorizzati, da una norma di legge o di regolamento, a riceverli;
5. devono rispettare scrupolosamente le misure di sicurezza, tecniche ed organizzative, nei trattamenti con strumenti elettronici e senza l'ausilio di strumenti elettronici (Allegato 3);
6. fermi restando gli obblighi e le responsabilità civili e penali dei dipendenti pubblici nell'ambito della loro attività, sono consapevoli che l'obbligo tassativo di attenersi alle misure di sicurezza riportate nell'Allegato 3 è sottoposto a vincolo disciplinare;
7. ai sensi degli articoli 29 e 32, comma 4 del Regolamento, dovranno prendere parte a specifici corsi di formazione in materia di trattamento dei dati.

All'atto dell'assunzione in servizio, verrà consegnata ad ogni nuovo componente, anche temporaneo, delle unità organizzative "Personale docente interno ed esterno" e "Assistenti educativi", copia della lettera di designazione ed i relativi allegati che sono parte integrante della lettera stessa.

Nell'ambito dei compiti previsti dall'art. 39 del Regolamento, l'osservanza delle disposizioni in materia di protezione dei dati personali da parte degli incaricati, è sorvegliata dal Responsabile della protezione dei dati personali, nella persona dell'ing. Marco Magazzeni.

L'elenco del personale designato è riportato nell'Allegato 4.

Il Dirigente Scolastico
Scotto Di Carlo Diego
Firma autografa omessa ai sensi degli artt. 3, comma 2°,
del d.lgs. n. 39 del 1993 e 47 del d.lgs. n. 82 del 2005.

Allegato 1

Elenco dei trattamenti effettuati dalle unità organizzative
"Personale docente interno ed esterno" e "Assistenti educativi"

Elenco dei trattamenti che comportano l'uso dei dati personali

T1 - Alunni	Dati personali trattati dai Docenti

Elenco dei trattamenti che comportano l'uso di dati sensibili e giudiziari
(D.M. 07.12.2006 n. 305)

Scheda n. 4	Attività propedeutiche all'avvio dell'anno scolastico
Scheda n. 5	Attività educativa, didattica e formativa, di valutazione
Scheda n. 7	Rapporti scuola - famiglie: gestione del contenzioso

Finalità del trattamento

1. Ai sensi dell'art. 6 del Regolamento, il trattamento dei dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
2. È vietata all'incaricato qualsiasi forma di comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati.

Modalità del trattamento

Il trattamento può essere effettuato manualmente, mediante strumenti informatici, telematici o altri supporti.
Ai sensi dell'art. 5 del Regolamento, i dati personali devono essere:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. esatti e, se necessario, aggiornati;
5. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
6. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Ai sensi degli articoli 9 e 10 del Regolamento, i dati sensibili e giudiziari devono essere trattati esclusivamente per motivi di interesse pubblico rilevante sulla base del diritto nazionale.
Il trattamento dei dati sensibili e giudiziari deve:

1. essere proporzionato alla finalità perseguita;
2. rispettare l'essenza del diritto alla protezione dei dati;
3. prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

I dati sensibili e giudiziari trattati e le relative operazioni effettuate sono riportati nel Decreto ministeriale 7 dicembre 2006 n. 305 (in allegato alla presente lettera di designazione) *"Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali"*.

Categorie di soggetti ai quali i dati possono essere comunicati

1. La comunicazione da parte dell'istituto ad altri soggetti pubblici e/o privati è ammessa quando è prevista da una norma di legge o di regolamento. Per i dati sensibili e giudiziari fare riferimento al Decreto ministeriale 7 dicembre 2006 n. 305;
2. Qualora non sia disciplinata da una norma di legge o di regolamento, fermo restando il rispetto delle finalità e delle modalità del trattamento, la comunicazione dei soli dati personali è autorizzata previo consenso informato dell'interessato.

Allegato 3

Misure tecniche e organizzative
(art. 32 del Regolamento)

Trattamenti con strumenti elettronici

Sistema di autenticazione informatica per il sistema operativo e i software di trattamento dati

1. **CREDENZIALI DI AUTENTICAZIONE**
   a) il trattamento dei dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
   b) le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;
   c) ad ogni incaricato sono assegnate individualmente le credenziali per l'autenticazione. Le credenziali di autenticazione sono assolutamente **personali** e **non cedibili**, per nessuna ragione;
   d) sono disattivate se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
   e) sono disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

2. **GLI INCARICATI DEVONO ADOTTARE LE NECESSARIE CAUTELE PER ASSICURARE LA SEGRETEZZA DELLA COMPONENTE RISERVATA DELLA CREDENZIALE E LA LORO DILIGENTE CUSTODIA**
   *In particolare gli incaricati **devono**:*
   a) utilizzare password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa da quella usata da sistemi "sicuri";
   b) porre in essere quanto riportato ai punti a), b), c) e d) relativi alla parola chiave,
   *mentre **non devono**:*
   a) comunicare ad altra persona la propria password (lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le proprie risorse o possa farlo a proprio nome);
   b) scrivere la propria password su fogli di carta che possono essere letti facilmente, ad esempio vicino al computer;
   c) immette la password quando c'è il rischio che qualcun altro possa leggere il contenuto sulla tastiera del computer;
   d) scegliere password che si possono trovare in un dizionario;
   e) credere che usare parole straniere renda più difficile il lavoro di scoperta;
   f) usare il proprio nome utente: è la password più semplice da indovinare;
   g) usare password in qualche modo legate alla propria persona come, ad esempio, il proprio nome, quello della moglie/marito, dei figli, del cane, date di nascita, numeri di telefono, etc..

3. **LA PAROLA CHIAVE:**
   a) deve essere composta da almeno otto caratteri (nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito) e deve essere alfanumerica;
   b) non deve contenere riferimenti agevolmente riconducibili all'incaricato;
   c) è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi;
   d) in caso di trattamento di dati sensibili e giudiziari la parola chiave è modificata almeno ogni tre mesi.

4. **PER NON LASCIARE INCUSTODITO E ACCESSIBILE LO STRUMENTO ELETTRONICO DURANTE UNA SESSIONE DI TRATTAMENTO, GLI INCARICATI DEVONO SVOLGERE ALMENO UNA DELLE SEGUENTI OPERAZIONI**
   a) terminare la sessione di lavoro al computer ogni volta che ci si deve allontanare, effettuando un log out o mettendo in atto accorgimenti tipo il blocco della sessione;
   b) un collega, che abbia lo stesso profilo autorizzativo nel trattamento dei dati, deve rimanere nella stanza durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;

c) chiudere a chiave la stanza dove è situato lo strumento elettronico durante l'assenza dell'incaricato, se nella stessa non rimane nessuno.

5. MODALITÀ CON LE QUALI IL TITOLARE ASSICURA LA DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI PROLUNGATA ASSENZA O IMPEDIMENTO DELL'INCARICATO CHE RENDA INDISPENSABILE E INDIFFERIBILE INTERVENIRE PER ESCLUSIVE NECESSITÀ DI OPERATIVITÀ E DI SICUREZZA DEL SISTEMA

il soggetto incaricato della custodia delle copie delle credenziali di ciascun incaricato è il DSGA dott.ssa Grazia Lo Iacono

a) per ciascun incaricato, la copia delle credenziali deve essere conservata in **busta chiusa munita di data, firma e sigillo** apposto direttamente dall'incaricato proprietario delle credenziali stesse;
b) le buste sono conservate in contenitore chiudibile a chiave, collocato a sua volta nell'armadio blindato dell'ufficio del DSGA;
c) in caso di assenza di un incaricato e di necessità ad operare un trattamento in sua vece, il DSGA autorizza l'apertura della busta e assegna l'operatività ad altro incaricato; contestualmente verrà data comunicazione all'interessato assente di quanto accaduto. Al ritorno di quest'ultimo, verrà ripristinata l'operatività originaria dopo che l'incaricato avrà rielaborato una nuova password e consegnato una copia delle credenziali aggiornate al DSGA.

6. I DATI PERSONALI SONO PROTETTI CONTRO IL RISCHIO DI INTRUSIONE E DELL'AZIONE DI PROGRAMMI DI CUI ALL'ART. 615-QUINQUIES DEL CODICE PENALE, MEDIANTE L'ATTIVAZIONE DI IDONEI STRUMENTI ELETTRONICI DA AGGIORNARE CON CADENZA ALMENO SEMESTRALE

1. i computer sono protetti dal programma antivirus **Microsoft Security Essentials** che è un antivirus freeware creato da Microsoft che difende i computer da virus, spyware, rootkit e trojan;
2. il programma antivirus viene aggiornato con cadenza **almeno trimestrale**;
3. la rete informatica e i programmi e applicativi che trattano dati sensibili e giudiziari sono protetti contro l'accesso abusivo ai sensi dell'art. 615-ter del Codice Penale attraverso l'installazione di idonei dispositivi elettronici (firewall e programmi denominati Intrusion Detection System, IDS).

Linee guida per la prevenzione dei virus informatici

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido o a catturare informazioni riservate (password/chiavi di sblocco, etc.).

Comportamenti che aumentano il rischio di contrarre un virus informatico:

a) utilizzo di supporti di memoria non personali ma di altri operatori;
b) uso di software gratuito o shareware scaricato da siti Internet o in allegato a riviste o libri;
c) uso di supporti di memoria preformattati;
d) collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido;
e) collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del server;
f) uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati;
g) uso di modem mentre si è connessi alla rete intranet aziendale protetta;
h) ricezione di applicazioni e dati dall'esterno (Amministrazioni, fornitori, ecc.);
i) utilizzo dello stesso computer da parte di più persone;
j) collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
k) collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
l) file attached di posta elettronica.

Comportamenti che riducono il rischio di contrarre un virus informatico:

a) utilizzare soltanto programmi provenienti da fonti fidate.
Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato ed autorizzato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus;
b) assicurarsi che il proprio software antivirus sia aggiornato.

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus;

c) non diffondere messaggi di provenienza dubbia.
   Se si ricevono messaggi che avvisano di un nuovo virus pericolosissimo, è necessario ignorarli: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle “leggende metropolitane” della rete;
d) non partecipare a "catene di S. Antonio" e simili.
   Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso;
e) limitare la trasmissione di file eseguibili (.com, .exe, .ovl, .ovr) e di sistema (.sys) tra computer in rete;
f) non utilizzare i server di rete come stazioni di lavoro;
g) non aggiungere mai dati o file a dispositivi contenenti programmi originali;
h) non condividere nessuna cartella del proprio computer ma utilizzare i file server o server ftp.

7. PROGRAMMI PER ELABORATORE VOLTI A PREVENIRE LA VULNERABILITÀ DEGLI STRUMENTI ELETTRONICI E A CORREGGERNE DIFETTI

1. sono adottati programmi che effettuano un aggiornamento costante dei prodotti, sistema operativo e applicazioni, non appena viene scoperto un bug, mediante installazione di patch che effettuano una verifica periodica dell’installazione e della configurazione dei prodotti software. L’aggiornamento periodico ha frequenza **almeno annuale** e, nel caso di trattamento di dati sensibili e giudiziari, **almeno semestrale**;
2. è adottato un sistema idoneo alla **registrazione degli accessi logici** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica dell’attività dell’amministratore di sistema. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell’evento che le ha generate e devono essere conservate per un congruo periodo, **non inferiore a sei mesi**.

8. ISTRUZIONI ORGANIZZATIVE E TECNICHE PER IL SALVATAGGIO DEI DATI CON FREQUENZA ALMENO SETTIMANALE

L’integrità dei **dati sul server** è garantita da una doppia procedura di back-up:

1. la prima avviene in automatico con apposito software che giornalmente opera il salvataggio di una copia dei dati sul server stesso;
2. la seconda è effettuata copiando su supporto rimovibile (CD-ROM), con cadenza settimanale, i back-up di tutta la settimana eseguiti sul server.

I supporti rimovibili (CD-ROM) vengono conservati nell’armadio blindato dell’ufficio del DSGA. Lo stesso contiene anche le copie di salvataggio degli applicativi.

A livello locale di **personal computer (client)** la procedura di back-up avviene:

1. mediante il software antivirus installato che opera il salvataggio automatico di una copia dei dati impostato settimanalmente;
2. copiando su supporto rimovibile (chiave USB) i dati, sempre con cadenza settimanale.

I supporti rimovibili sono custoditi nell’armadio blindato dell’ufficio del DSGA.

I supporti rimovibili contenenti **dati sensibili e giudiziari** se non utilizzati vengono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, solo dopo aver reso le informazioni in essi contenuti non intelligibili e tecnicamente in alcun modo ricostruibili.

9. ISTRUZIONI TECNICHE E ORGANIZZATIVE PER LA CUSTODIA E L’USO DEI SUPPORTI RIMOVIBILI

Al fine di evitare accessi non autorizzati e trattamenti non consentiti, i supporti rimovibili (CD-ROM e

chiavi USB) su cui sono memorizzati i dati, sono:

1. custoditi nell'armadio blindato dell'ufficio del DSGA al termine della giornata lavorativa;
2. conservati in cassetti chiusi a chiave durante il loro utilizzo. Inoltre devono essere eseguite le disposizioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, di cui al punto 7 delle Misure tecniche e organizzative - Trattamenti con strumenti elettronici;
3. formattati quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi. Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

10. MISURE PER GARANTIRE IL RIPRISTINO DELL'ACCESSO AI DATI IN CASO DI DANNEGGIAMENTO DEGLI STESSI O DEGLI STRUMENTI ELETTRONICI

1. La procedura di salvataggio periodico avviene mediante il software di back-up del programma di gestione amministrativa il quale crea in automatico, con cadenza giornaliera, una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e di un masterizzatore *DVD* che salva i back-up di tutta la settimana su disco *DVD* registrabile, da utilizzare al termine della giornata lavorativa del venerdì.
2. Al termine della settimana lavorativa i singoli incaricati provvederanno ad effettuare il salvataggio dei dati su chiave *USB*. I supporti rimovibili sono custoditi all'interno dell'armadio blindato dell'ufficio del DSGA.
3. Il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento avverrà mediante l'utilizzo degli appositi back-up operati dai singoli incaricati.
   NOTE:
   a) *Il server è collegato ad un gruppo di continuità statico UPS che entra in funzione in seguito alla mancanza di corrente elettrica o a causa di sbalzi di tensione.*
   b) *I computer, incluso il server, sono sollevati da terra in modo da evitare eventuali perdite di dati dovuti ad allagamenti.*

11. MISURE DI SICUREZZA ESEGUITE DA SOGGETTI ESTERNI ALLA STRUTTURA

I soggetti esterni all'istituto scolastico (Amministratore di sistema, installatori, società di software e hardware, ecc.) che eseguono, per conto del titolare del trattamento, le misure minime di sicurezza riportate nei punti precedenti, devono presentare una **descrizione scritta dell'intervento effettuato** che ne attesti la conformità alle disposizioni di sicurezza adottate dall'istituto scolastico.

Trattamenti senza l'ausilio di strumenti elettronici

1. **DISPOSIZIONI COMUNI**
   1. Alla presa in carico di un atto o un documento cartaceo contenente dati personali, l'incaricato è responsabile della custodia del documento e dovrà controllarlo, fino ad avvenuta restituzione, affinché personale non autorizzato non venga in qualche modo a conoscenza del contenuto del documento stesso;
   2. Le attrezzature e i dispositivi sui quali è possibile trovare materiale cartaceo contenente dati personali (archivi, armadi, scaffalature, scrivanie, stampanti, ecc.) sono ubicati in modo tale che ciascun addetto al trattamento possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee non autorizzate;
   3. Gli incaricati al trattamento, in collaborazione con i collaboratori scolastici, non devono consentire al personale non autorizzato di leggere o prelevare documenti non ancora presi in carico, in corrispondenza di stampanti, apparecchi telefax, scrivanie, scaffali, ecc.;
   4. I documenti contenenti dati acquisiti attraverso il protocollo riservato sono conservati nell'armadio blindato collocato nell'ufficio del DSGA.

2. **TRATTAMENTO DEI DATI PERSONALI IDENTIFICATIVI**
   1. i documenti cartacei contenenti dati personali identificativi sono conservati in armadi e scaffalature all'interno di uffici/stanze chiudibili a chiave;
   2. al termine della giornata lavorativa, anche se dovranno essere riutilizzati nei giorni successivi, i documenti devono essere riposti all'interno dell'armadio/scaffalatura di provenienza e la stanza chiusa a chiave.

3. **TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI**
   1. i documenti cartacei contenenti dati sensibili e giudiziari sono conservati in armadi dotati di serratura all'interno di uffici/stanze chiudibili a chiave;
   2. quando affidati agli incaricati per lo svolgimento dei relativi compiti, gli atti e i documenti contenenti dati sensibili e giudiziari **sono controllati e custoditi** dagli stessi incaricati fino alla loro restituzione, in maniera che ad essi non accedano persone prive di autorizzazione al trattamento;
   3. al termine della giornata lavorativa, anche se dovranno essere riutilizzati nei giorni successivi, i documenti devono essere riposti all'interno dell'armadio di provenienza e la stanza chiusa a chiave;
   3. l'accesso agli archivi contenenti dati sensibili e giudiziari **è controllato**. Le persone ammesse agli archivi, a qualunque titolo, dopo l'orario di servizio, vengono identificate e registrate su apposito registro (le disposizioni sono contenute nella lettera di incarico dell'unità organizzativa "collaboratori scolastici").

Nome: …….

Cognome: ……

Firma per accettazione

……

Roma ……..

CONSENSO INFORMATO PER L'UTILIZZO
DELLA PIATTAFORMA GOOGLE SUITE FOR EDUCATION
(ai sensi dell'art. 7 del GDPR "Regolamento UE 679/2016 sulla protezione dei dati")

Al Titolare del trattamento
Dirigente scolastico Istituto Comprensivo Castelverde
Nicola Armignacca
e-mail: rmic8cp00e@istruzione.it
PEC: rmic8cp00e@pec.istruzione.it

Il/la sottoscritto/a ……. nato/a a ……. il ……..
facente parte dell'unità organizzativa dell'istituto Comprensivo Castelverde *(indicare con una X l'unità organizzativa di appartenenza)*:

1. collaboratore del DS (….);
2. personale ATA (….);
3. personale docente (….);
4. assistente educativo (….);
5. organo collegiale (….),

AUTORIZZA

l'istituto Comprensivo Castelverde al trattamento dei propri dati nell'ambito dell'utilizzo della piattaforma Google Suite for Education, secondo quanto indicato nell'informativa in allegato alla presente, ai sensi dell'articolo 14 del GDPR 679/16.

Roma, Lì ……..

Firma dell'interessato

……..

Ministero dell'Istruzione – Ufficio Scolastico Regionale per il Lazio

Istituto Comprensivo Castelverde

www.iccastelverderoma.edu.it

Via Massa di San Giuliano, 131 – 00132 ROMA Tel. 06 455 90 500
PEO: rmic8cp00e@istruzione.it - PEC: rmic8cp00e@pec.istruzione.it
Codice meccanografico: RMIC8CP00E Codice fiscale: 97616500589
IPA - Codice univoco ufficio per Fatturazione Elettronica: UFEHD1

DICHIARAZIONE FORMAZIONE IN TEMA DI SICUREZZAE TRASMISSIONE COPIA ATTESTATI

Il/La sottoscritto/a_____,in servizio presso codesta istituzione scolastica con la qualifica di_____con contratto _____ , consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere, di formazione o uso atti falsi richiamate dall'art.76 del D.P.R 445 del dicembre 2000, nonché della sanzione ulteriore prevista dall'art. 75(3) del citato D.P.R. 445 del 28 dicembre 2000, così come modificato ed integrato dall'art 15 della legge 16/01/2003 n. 3, consistente nella decadenza dai benefici eventualmente conseguenti al provvedimento emanato sulla base della dichiarazione non veritiera,

DICHIARO/A

di aver frequentato i seguenti corsi di formazione in tema di sicurezza e igiene nei luoghi di lavoro ai sensi del D. Lgs 81/2008 e ss.mm.ii e di essere in possesso dei rispettivi attestati.

Tipologia corso	**Frequenza Si/No**	**Data**	**Ente che ha rilasciato l'attestato Se (si)**	**Aggiornamento n. ore**	**Data**	**Ente che ha rilasciato l'attestato Se (si)**
Corso di **formazione per i Lavoratori formazione generale** durata 4 ore						
Corso di **formazione per i Lavoratori formazione specifica** durata 8 ore						
Corso di formazione per **Addetto del Servizio diPrevenzione e Protezione (A.S.P.P.) modulo A** durata 30 ore						

Corso di formazione per **Addetto del Servizio di Prevenzione e Protezione (A.S.P.P.) modulo B** durata 26						
Corso di formazione per **Responsabile del Servizio di Prevenzione e Protezione (R.S.P.P.) modulo C** durata 24 ore						
Corso di **formazione per Preposto** formazione aggiuntiva a quella dei lavoratori (12h) durata 8 ore						
Corso per **Addetto antincendio** per attività arischio medio durata 8 ore						
Attestato di idoneità tecnica per addetti antincendio in scuole con oltre 300 presenzerilasciato dal Comando dei VV.F.						
Corso per **Addetto di Primo Soccorso** durata 12 ore						
Corso di **formazione Rappresentanti lavoratori per la sicurezza (R.L.S.)** durata 32 ore						

A corredo della presente dichiarazione il sottoscritto

- allega
- trasmetterà entro 15 giorni

le copie dei corrispondenti attestati dei corsi di formazione effettuati.

Dichiaro di essere informato, ai sensi e per gli effetti di cui al GDPR 679/2016, che i dati personali raccolti saranno trattati, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa.

Roma ……..

In fede

…….