LICEO ARTISTICO STATALE "BRUNO MUNARI"
VIA GANDHI 14 – 31029 VITTORIO VENETO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

ALLEGATO A

NATURA E LUOGHI DI RESIDENZA DEI DATI, FINALITÀ E MODALITÀ DEL TRATTAMENTO AUTORIZZATI, TIPOLOGIE DI COMUNICAZIONE E DIFFUSIONE AMMESSE

1. **Personale amministrativo**
   - Banca Dati: ALUNNI
   - Banca Dati: PERSONALE
   - Banca Dati: CONTABILITA'
   - Banca Dati: FORNITORI DI BENI E SERVIZI
   - Banca Dati: PROTOCOLLO
2. **Personale docente**
3. **Collaboratori scolastici**

Firma del Responsabile del Trattamento …….

PERSONALE AMMINISTRATIVO

Banca Dati: ALUNNI

1. FONTE NORMATIVA

   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. FINALITA' TRATTAMENTO:
   - attività propedeutiche all'avvio dell'anno scolastico,
   - attività educativa, didattica, di valutazione,
   - attività di orientamento e certificazione delle competenze,
   - gestione del contenzioso (reclami, esposti, ricorsi, provvedimenti disciplinari, ect.)
   - attivazione di organismi collegiali;
   - attività didattica relativa a situazione di handicap.

3. MODALITA' DI TRATTAMENTO DEI DATI:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (v. titolario) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato al titolario	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. NATURA DEI DATI:
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

   Sono da considerare dati sensibili:

- origini razziali ed etniche,
- convinzioni religiose ed adesione ad organizzazione a carattere religioso,
- stato di salute,
- convinzioni politiche,
- dati giudiziari

e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. COMUNICAZIONE E DIFFUSIONE:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - 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 istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad 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 del D. Lgsl. 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 ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.
6. LUOGHI OVE RESIEDONO I DATI

   Archivio cartaceo:
   - Archivio storico;
   - Ufficio della Didattica nell'archivio corrente (schedari, armadi, computers);
   - Ufficio del DSGA (armadi e armadio blindato)

   Archivio informatico

Banca Dati: PERSONALE

1. FONTE NORMATIVA

   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. FINALITA' TRATTAMENTO:
   - Trattamento giuridico ed economico del personale e dei collaboratori esterni
   - Gestione previdenziale e pensionistica
   - Reclutamento, selezione, valutazione e monitoraggio del personale
   - Aggiornamento e formazione professionale
   - Adempimento di obblighi fiscali e contabili
   - Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali
   - Gestione del contenzioso e dei procedimenti disciplinari
   - Attivazione di organismi collegiali.
   - gestione dati inerenti lo stato di salute per esigenze amministrative del personale, assunzioni del personale appartenente alle c.d. categorie protette, igiene e sicurezza sul luogo di lavoro, equo indennizzo, cause di servizio ecc.,

3. MODALITA' DI TRATTAMENTO DEI DATI:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (cartelle del personale) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato alle cartelle	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. NATURA DEI DATI:
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).

- Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

Sono da considerare dati sensibili:

- origini razziali ed etniche,
- convinzioni religiose ed adesione ad organizzazione a carattere religioso,
- stato di salute,
- convinzioni politiche,
- dati giudiziari

e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. COMUNICAZIONE E DIFFUSIONE:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - 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 istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad 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 del D. Lgsl. 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 ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.
6. LUOGHI OVE RESIEDONO I DATI

   Archivio cartaceo:
   - Archivio storico;
   - Ufficio del Personale nell'archivio corrente (schedari, armadi, computers);
   - Ufficio del DSGA (armadi e armadio blindato)

   Archivio informatico

Banca Dati: CONTABILITA'

1. FONTE NORMATIVA

   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. FINALITA' TRATTAMENTO:
   - Trattamento giuridico ed economico del personale e dei collaboratori esterni
   - Gestione stipendiale e previdenziale
   - Aggiornamento e formazione professionale
   - Adempimento di obblighi fiscali e contabili
   - Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali
   - gestione contratti esperti esterni
   - gestione per le negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni
   - gestione di incassi e pagamenti.

3. MODALITA' DI TRATTAMENTO DEI DATI:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (v. cartelline del personale) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato alle cartelline del personale	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. NATURA DEI DATI:
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

Sono da considerare dati sensibili:

- origini razziali ed etniche,
- convinzioni religiose ed adesione ad organizzazione a carattere religioso,
- stato di salute,
- convinzioni politiche,
- dati giudiziari

e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. COMUNICAZIONE E DIFFUSIONE:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - 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 istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad 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 del D. Lgsl. 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 ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.
6. LUOGHI OVE RESIEDONO I DATI

   Archivio cartaceo:
   - Archivio storico;
   - Ufficio della contabilità nell'archivio corrente (schedari, armadi, computers);
   - Ufficio del DSGA (armadi e armadio blindato)

   Archivio informatico

Banca Dati: FORNITORI DI BENI E SERVIZI

1. FONTE NORMATIVA

   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

2. FINALITA' TRATTAMENTO:
   - Adempimenti di obblighi fiscali e contabili
   - Gestione documenti di trasporto, fatture e note accredito;
   - Gestione richieste preventivi e offerte a fornitori attivi e/o potenziali
   - Gestione fornitori.

3. MODALITA' DI TRATTAMENTO DEI DATI:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (registri) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato ai registri	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

4. NATURA DEI DATI:
   - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
   - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
   - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
   - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
   - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

   Sono da considerare dati sensibili:
   - origini razziali ed etniche,
   - convinzioni religiose ed adesione ad organizzazione a carattere religioso,
   - stato di salute,
   - convinzioni politiche,
   - dati giudiziari

   e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

5. COMUNICAZIONE E DIFFUSIONE:
   - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
   - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
   - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
   - 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 istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
   - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
   - ad 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 del D. Lgsl. 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 ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
   - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
   - particolari forme di trattamento e operazioni eseguite.
6. LUOGHI OVE RESIEDONO I DATI

   Archivio cartaceo:
   - Archivio storico;
   - Ufficio della Contabilità nell'archivio corrente (schedari, armadi, computers);
   - Ufficio del DSGA (armadi e armadio blindato)

   Archivio informatico

Banca Dati: PROTOCOLLO

7. FONTE NORMATIVA

   T.U. 16.4.1994 n.297, T.U. artt. 309 e 310, D.P.R.22.12.1967 n.1518, D.P.R. 26.1.1999 n.355, Legge 5.2.1992 n.104, D.P.R. 31.8.1999 n.394, D.P.R. 24.7.1977 n.616, L.5.6.1930 n.824, D.P.R. 12.2.1985 n.104, D.P.R. 21.7.1987 n.339

8. FINALITA' TRATTAMENTO:
   - Istruzione ed assistenza scolastica
   - amministrazione di studenti
   - organizzazione dell'attività di insegnamento e valutazione, assistenza, anche ai fini di orientamento e ai fini professionali
   - sussidi, borse e assegni, ecc.

9. MODALITA' DI TRATTAMENTO DEI DATI:

	In forma cartacea	*In forma elettronica*
1. Raccolta	- presso gli interessati - presso terzi - tramite schede - per via telefonica - presso registri, elenchi, atti o documenti pubblici	- per via telematica
2. Registrazione	- su supporto cartaceo	- su supporto elettronico (server, CD rom, dischetti, …)
3. Organizzazione	- aggregazione di dati - elaborazione in forma cartacea - trasformazione in forma anonima - creazione di profili	- aggregazioni di dati - elaborazione in forma elettronica - trasformazione in forma anonima - creazione di profili
4. Conservazione / modifica	- in archivi cartacei (registri) chiusi a chiave	- in archivi elettronici (ND, CD, FD) protetti da password
5. Consultazione / estrazione / utilizzo	- accesso autorizzato ai registri	- accesso con credenziale all'archivio elettronico
6. Cancellazione / distruzione	- utilizzo degli appositi distruggi documenti	- eliminazione dei dischetti usati per archiviare dati sensibili e giudiziari

10. NATURA DEI DATI:
    - Nominativo indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita; indirizzo privato, indirizzo di lavoro, numero di telefono o di fax o posta elettronica; posizioni rispetto agli obblighi militari; numero di carta di identità, passaporto,patente di guida; numero di posizione previdenziale o assistenziale).
    - Codice fiscale ed altri numeri di identificazione personale (carte sanitarie).
    - Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al gruppo famigliare).
    - Lavoro (occupazione attuale, precedente; informazione sulla formazione professionale; curriculum lavorativo, competenze professionali).
    - Istruzione e cultura (curriculum di studi e accademico; titolo di studio).

    Sono da considerare dati sensibili:
    - origini razziali ed etniche,
    - convinzioni religiose ed adesione ad organizzazione a carattere religioso,
    - stato di salute,
    - convinzioni politiche,
    - dati giudiziari

e quindi da conservare in archivi separati e chiusi a chiave se cartacei o protetti da particolare credenziale di autenticazione se elettronici.

11. COMUNICAZIONE E DIFFUSIONE:
    - agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
    - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
    - alle USL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la preparazione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
    - 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 istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
    - all'INAIL per la denuncia di infortuni ex D.P.R. 30 giugno 1965, n. 1124;
    - ad 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 del D. Lgsl. 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 ed amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione giudiziaria;
    - ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza;
    - particolari forme di trattamento e operazioni eseguite.
12. LUOGHI OVE RESIEDONO I DATI

    Archivio cartaceo:
    - Archivio storico;
    - Ufficio della Contabilità nell'archivio corrente (schedari, armadi, computers);
    - Ufficio del DSGA (armadi e armadio blindato)

    Archivio informatico

PERSONALE DOCENTE

I dati personali e/o sensibili trattati dai docenti sono:

- i dati personali comuni utilizzati per l'attività didattica e/o organizzativa
- i dati particolari quali quelli deducibili da:
- informazioni contenute nelle comunicazioni scuola –famiglia;
- motivazione assenze per motivi familiari e/o personali;
- note disciplinari trascritte nei trascritte nei registri di classe o nei provvedimenti di sospensione, ecc. (dato particolare in quanto la sua diffusione potrebbe ledere la dignità dell'interessato e il suo diritto alla riservatezza);
- valutazioni intermedie e finali, nonché votazioni, sul profitto, il grado di impiego, la condotta, di ogni alunno assegnato (dati particolari la cui diffusione potrebbe ledere la dignità dell'interessato e il suo diritto alla riservatezza);
- elaborati scritti, in particolare temi di italiano riportati in taluni casi informazioni delicate sulla sfera personale e familiare (dati particolari di grado elevato).

Sono dati sensibili quelli relativi a:

- scelta dell'alunno di avvalersi dell'insegnamento della Religione Cattolica (dati sensibili in quanto idonei a rilevare con buona probabilità le convinzioni religiose);
- giustificazioni di assenze dovute a festività religiose non cattoliche (festività ebraiche, ecc.): dato sensibile in grado di rilevare la convinzione religiosa;
- giustificazione di assenze dovute a motivi di salute (in quanto in taluni casi idoneo a rilevare parzialmente lo stato di salute) visione di certificati medici di avvenuta guarigione (dato particolare o sensibile in quanto parzialmente idoneo a rilevare lo stato di salute);
- certificazioni mediche per esonero da educazione fisica con diagnosi (dato sensibile in quanto idoneo a rivelare lo stato di salute);
- documentazione per l'integrazione di alunni disabili (dato sensibile in quanto idoneo a rilevare lo stato si salute).

Costituiscono occasioni di trattamento dei dati da parte dei docenti quelle in cui essi sono chiamati a:

1. gestire:
   - registri di classe, contenenti dati comuni e particolari (certificati medici contenuti in una busta nell'ultima pagina del registro);
   - registro del docente in cui sono annotati dati comuni e particolari;
   - registro dei verbali dei Consigli di Classe (dati di tipo comune e particolari), normalmente conservato a cura del Responsabile del trattamento in armadio chiuso a chiave, quando esso è affidato al verbalizzatore e/o al coordinatore di classe;
   - registri e i documenti in occasione di esami e concorsi;
   - elenchi di alunni, dipendenti e genitori per attività varie della scuola;
   - dati comuni degli alunni in caso di visite d'istruzione o viaggi.
2. trattare dati personali in occasione della partecipazione a:
   - commissioni scolastiche;
   - all'organizzazione delle elezioni degli organi collegiali (dati comuni);
   - ad attività di gestione del sindacato interno, con conoscenza di dati anche sensibili;
   - alla realizzazione delle attività previste dal POF;
   - rapporti di continuità nel passaggio degli studenti da un Istituto all'altro.

Per quanto riguarda le modalità di raccolta dei dati si precisa che essi provengono:

- dall'ufficio di segreteria o dalla visione di dati presenti nel Fascicolo Personale detenuto dalla scuola;
- da comunicazioni scritte dalla famiglia o da comunicazioni verbali dello studente;
- dai certificati medici (in casi di esonero da Educazione Fisica) forniti dell'ufficio di segreteria;
- da certificati medici di giustificazione delle assenze esibiti dallo studente stesso;
- da elaborati, forniti direttamente dall'interessato.

I documenti che contengono i dati trattati dai docenti sono conservati in aula docenti, in contenitori chiusi con chiave custodita dal singolo docente autorizzato allo specifico trattamento.

COLLABORATORI SCOLASTICI

I dati personali e/o sensibili trattati dai collaboratori scolastici sono quelli contenuti nei documenti che essi sono incaricati di ricevere, trasportare, consegnare, inviare aperti o collocati in busta chiusa, in particolare:

a. elenchi di alunni, dipendenti e genitori per attività varie della scuola;
b. certificati medici contenuti nella busta allegata al registro di classe che al termine delle lezioni vengono consegnati ai collaboratori scolastici; questi li pongono nell'armadio destinato alla loro custodia, mentre il registro viene riposto, in custodia, negli scaffali del bancone del centralino;
c. dati personali che sono visionati allo scopo di dare indicazioni di massima agli utenti.

Costituiscono occasione di trattamento dei dati da parte dei collaboratori scolastici quelle in cui essi sono chiamati a svolgere attività di supporto a tutti i trattamenti svolti nella scuola e in particolare:

a. custodire documenti e registri per brevi periodi
b. fotocopiare e faxare documenti contenenti dati personali
c. collaborare ad operazioni di archiviazione di documenti cartacei e/o imputazione di dati negli archivi elettronici.
d. collaborare ad operazioni di scarto ed eliminazione di documenti cartacei
e. collaborare alla gestione di tutti gli archivi cartacei dislocati lontano dalla segreteria.

I documenti che contengono i dati trattati dai collaboratori scolastici sono conservati negli armadi, schedari, contenitori in genere situati in portineria e chiusi a chiave.

LICEO ARTISTICO STATALE "BRUNO MUNARI"
VIA GANDHI 14 – 31029 VITTORIO VENETO

LINEE GUIDA IN MATERIA DI SICUREZZA DEI DATI

ALLEGATO B

1. **Istruzioni operative per la sicurezza dei dati – Personale Docente, amministrativo, tecnico e collaboratore scolastico**
2. **Disciplinare interno per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica da parte del personale e degli studenti**

Firma del Titolare del Trattamento ……

Firma del Responsabile del Trattamento ……

ISTRUZIONI OPERATIVE PER LA SICUREZZA DEI DATI

Questo documento fornisce agli incaricati del trattamento informazioni sulle loro responsabilità rispetto alla gestione ed alla sicurezza dei dati trattati dall'Istituto in particolare riguardo:

Integrità: le informazioni devono essere esatte ed aggiornate e non alterabili da incidenti o abusi;

Riservatezza: prevenzione contro l'accesso non autorizzato alle informazioni, quindi i trattamenti devono essere leciti e conformi alle finalità della raccolta;

Disponibilità: il sistema deve essere protetto da interruzioni impreviste e perdite di informazioni.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; nel momento in cui le informazioni raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Per garantire sicurezza cioè integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta il personale docente ed ATA uniforma il proprio comportamento professionale alle indicazioni sotto impartite.

Profilo: PERSONALE DOCENTE

Incaricato del trattamento dei dati sotto elencati è individuato l'intero corpo insegnante. Pertanto ogni docente, nel momento in cui è assegnato a far parte del corpo insegnante diventa automaticamente Incaricato di tali trattamenti e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. Al fine di garantire il diritto alla protezione dei dati e all'identità personale, nel trattamento dei dati i docenti sono tenuti a:
   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.

2. Al fine di garantire il diritto alla riservatezza i docenti si adoperano per:

   a. Prevenire la diffusione illecita di dati personali e sensibili, avendo cura di accedere ai soli dati, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico.

   b. Custodire i dati trattati con mezzi non elettronici avendo cura di:
      - conservare i documenti o atti che contengono dati personali o sensibili o giudiziari in contenitori chiusi a chiave;
      - distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
      - non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;
      - non lasciare incustoditi i registri didattici nonché inibirne la consultazione a terzi non autorizzati;
      - conservare i registri didattici nell'apposito armadietto avendo cura di chiuderlo a chiave. Data la natura pubblica di tale documento esso deve essere sempre aggiornato, e a disposizione del Dirigente Scolastico che può in ogni momento prenderne visione e quindi deve essere conservata, con la dovuta cautela, la chiave di riserva dell'armadietto stesso dal Responsabile del trattamento.
      - raccogliere nel registro di classe, in un'apposita busta chiusa apposta nell'ultima pagina di tale registro, i certificati medici che vengono utilizzati per giustificare le assenze. Durante l'orario delle lezioni questi registri sono in classe sulla scrivania, affidati all'insegnante di turno. Al termine delle lezioni un collaboratore scolastico, incaricato del trattamento, raccoglie i certificati medici contenuti nella busta e li ripone nell'armadio con chiave destinato alla loro custodia, mentre il registro viene riposto, in custodia, negli scaffali del bancone del centralino;
      - consultare e poi restituire alla segreteria i certificati medici per esonero da educazione fisica o limitazione dell'attività e in genere i certificati medici e altri documenti, di natura sensibile e non, relativi a particolari interventi didattici e all'integrazione di alunni portatori di handicap.
      - custodire in archivio sicuro gli elaborati degli studenti nei casi contenessero dati particolari. Nel caso si tratti di dati sensibili, consegnarli in busta chiusa alla segreteria per una conservazione a parte.

   c. Custodire i dati trattati elettronicamente avendo cura di seguire il **Disciplinare interno** per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica.

   d. Prevenire la comunicazione illecita di dati personali avendo cura di:
      - mantenere il riserbo su informazioni ricevute oralmente;
      - non fornire dati e informazioni di carattere sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario;
      - evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;
      - qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente.

3. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali è necessario comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori.

Profilo: ASSISTENTE AMMINISTRATIVO

Incaricato del trattamento dei dati sottoelencati è l'unità organizzativa denominata "assistenti amministrativi". Pertanto ogni unità di personale, nel momento in cui è assegnata a tale ruolo diventa automaticamente incaricata del trattamento, manuale o mediante strumenti informatici, e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. Al fine di garantire il diritto alla protezione dei dati e all'identità personale

   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati su richiesta degli interessati o comunque quando a conoscenza della variazione.

2. Al fine di garantire il diritto alla riservatezza

   - prevenire la diffusione illecita di dati personali sensibili avendo cura di accedere ai soli dati personali, oggetto di trattamento e la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico.

   - custodire i dati trattati su formato cartaceo avendo cura di:
     a. prelevare dagli archivi i soli atti e documenti necessari,
     b. conservare i documenti nelle attrezzature d'ufficio dotate di serratura e regolarmente chiuse, durante l'intero svolgimento delle operazioni di trattamento;
     c. conservare i documenti o atti che contengono dati sensibili o giudiziari separatamente, in archivi separati (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave e nei quali devono essere riposti al termine della giornata di lavoro e sempre prima di assentarsi dal posto di lavoro, anche se temporaneamente ed anche qualora l'incaricato debba continuare ad utilizzarli in periodi successivi;
     d. distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
     e. non lasciare dischetti, fogli, cartelle e quanto altro a disposizione di estranei;
     f. restituire prontamente all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative al termine del trattamento;

   - custodire i dati trattati elettronicamente avendo cura di seguire il **Disciplinare interno** per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica.

   - prevenire la comunicazione illecita di dati personali avendo cura di:
     a) non fornire dati e informazioni di carattere sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario;
     b) evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi di inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;
     c) qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente.

3. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali:
   a) comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori;
   b) aggiornare il registro di carico e scarico per la registrazione delle richieste di comunicazione della documentazione, contenente dati sensibili.

Profilo: COLLABORATORI SCOLASTICI

Incaricato del trattamento dei dati sotto elencati è l'unità organizzativa denominata "collaboratori scolastici". Pertanto ogni unità di personale, nel momento in cui è assegnata a tale ruolo diventa automaticamente incaricata del trattamento e riceve dal Responsabile del trattamento le istruzioni scritte sotto impartite:

1. A fine di garantire il diritto alla protezione dei dati e all'identità personale, i collaboratori scolastici nel trattamento dei dati sono tenuti a:
   - procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
   - procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.
2. Al fine di garantire il diritto alla riservatezza i collaboratori scolastici si preoccupano di:

   - prevenire la diffusione illecita di dati personali sensibili avendo cura di:
     a. accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
     b. impedire l'ingresso nei locali che sono stati loro affidati in custodia di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento, ricordando che:
        - al di fuori dell'attività lavorativa i locali adibiti ad ufficio devono essere chiusi a chiave;
        - durante l'orario di apertura degli uffici il normale livello di vigilanza è svolto dal personale in servizio;
        - l'accesso agli uffici è consentito solo al personale dipendente nei tempi e nei modi stabiliti dal DS.
        - gli utenti esterni (alunni, genitori, ecc.) non possono accedere all'area degli uffici se non accompagnati da personale dipendente;
        - i locali adibiti ad archivio devono essere chiusi a chiave anche durante l'attività lavorativa e il solo personale amministrativo è autorizzato ad accedere agli archivi;
        - tenere chiuso a chiave il locale dei server e consentire l'accesso solo alle persone incaricate dal responsabile del trattamento o dall'amministratore di sistema;
     c. impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che sono stati affidati loro in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del Trattamento;

   - custodire i dati trattati con mezzi non elettronici avendo cura di:
     a. conservare i documenti o atti che contengono dati sensibili o giudiziari negli archivi (stanze, armadi, schedari, contenitori in genere) individuati e chiusi a chiave secondo le istruzioni impartite dal Responsabile del trattamento;
     b. distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei, non più utilizzati;
     c. non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;
     d. non lasciare incustoditi i registri didattici ricevuti in temporanea consegna nonché inibirne la consultazione a terzi non autorizzati;

   - prevenire la comunicazione illecita di dati personali facendo attenzione a:
     a. non fornire dati e informazioni di carattere personale o sensibile per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario e la legittimità della richiesta;
     b. evitare di inviare per fax documenti in chiaro contenenti dati sensibili, nel caso sostituire il nome del soggetto interessato con codice identificativo e quindi inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato;
     c. qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante, quindi richiamare avendo così la certezza sull'identità del richiedente;

   4. Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali comunicare per iscritto al Responsabile del Trattamento eventuali difformità dei dati trattati o nel funzionamento degli elaboratori.

DISCIPLINARE INTERNO PER L'UTILIZZO DELLE STRUMENTAZIONI INFORMATICHE, DELLA RETE INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEL PERSONALE E DEGLI STUDENTI

Premesso che compete al datore di lavoro:

- assicurare la funzionalità delle strumentazioni informatiche in dotazione all'Istituto;
- adottare idonee misure di sicurezza per garantire la disponibilità e l'integrità dei sistemi informativi e dei dati, nonché per prevenire utilizzi indebiti;
- adottare limiti e cautele per evitare la registrazione e diffusione di fotografie e i filmati in tempo reale anche utilizzando i terminali di nuova generazione applicati alla telefonia mobile;
- indicare in modo particolareggiato quali siano gli strumenti messi a disposizione le modalità di utilizzo nell'organizzazione dell'attività lavorativa e/o di studio degli strumenti messi a disposizione dei dipendenti e degli studenti ritenute corrette;
- precisare in che misura e con quali modalità vengano effettuati i controlli;
- tutelare i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia;
- tener conto della normativa in tema di informazione, concertazione e consultazione delle organizzazioni sindacali,

sono stabilite le prescrizioni del presente disciplinare di seguito riportate che si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati del trattamento dati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) e a cui devono attenersi tutti gli utilizzatori (personale e studenti, d'ora in poi definiti *utenti*) delle strumentazioni informatiche, della rete internet e della posta elettronica.

Art. 1. Finalità

Il presente regolamento disciplina le modalità di accesso e di uso della Rete Informatica, telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo, documentario, alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Art. 2. Ambito di applicazione

La Rete del Liceo Artistico Statale "Bruno Munari" è costituita dall'insieme delle Risorse informatiche, cioè

- dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete Informatica dell'Istituto
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli *utenti* interni (personale amministrativo, docenti e collaboratori scolastici) autorizzati ad accedere alla Rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria nonché agli studenti nei limiti loro assegnati.

Analogamente il presente regolamento si applica alle ditte che effettuano attività di manutenzione, agli eventuali altri soggetti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle convenzioni stesse nel rispetto del presente disciplinare tecnico e a tutti i collaboratori dell'Istituto a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetto in stage, ecc.).

Art. 3. Principi generali

IL Liceo Artistico Statale "Bruno Munari" prevede l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica da parte degli *utenti* quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

1. *principio di necessità*: i sistemi informativi e I programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;

2. *principio di correttezza*: le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori;
3. *principio di pertinenza e non eccedenza*: i trattamenti sono effettuati per finalità determinate, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.

Art. 4. Valutazione del rischio

La rete informatica di Istituto, l'accesso alla rete internet e alla posta elettronica, il PC affidato al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e backup ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In relazione all'utilizzo non corretto di detti strumenti si individuano I seguenti possibili rischi e conseguenti effetti:

Attività	Rischio	Motivazione	Possibile effetto
Manutenzione di periferiche a hardware interne (scheda video, memoria, ecc.)	Alto	Possono essere danneggiati componenti interni e il PC	Danneggiamento dei PC
Manutenzione di periferiche a hardware esterne (tastiere, mouse, ecc.)	Basso		
Download non controllato o non programmato di update o upgrade di applicazioni installate dal responsabile di rete	Alto	Possono essere scaricate applicazioni non verificate con il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.	Danneggiamento dei PC o della rete informatica interna per incompatibilità con il software esistente
Download controllato o programmato di update o upgrade di applicazioni installate dal responsabile di rete	Basso		
Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.)	Alto	Possono essere scaricate applicazioni non verificate con il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.	Danneggiamento dei PC o della rete informatica interna Gravi responsabilità civili ed anche penali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore sul software
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	Alto	Possono essere installate applicazioni non verificate	Danneggiamento dei PC o della rete informatica interna
Accesso alla rete esterna	Medio	Possono presentarsi attacchi da applicazioni nella rete esterna	Danneggiamento dei PC o della rete informatica interna
Download delle e-mail	Basso		
Apertura di allegati di posta elettronica di incerta provenienza	Alto	Possono presentarsi attacchi da applicazioni nella rete esterna	Danneggiamento dei PC o della rete informatica interna. Divulgazione di password
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	Alto	Possibile utilizzo da parte di terzi, che in seguito non sarebbe possibile provare.	Uso indebito di dati riservati, danneggiamento della rete informatica

			interna.
Utilizzo di supporti removibili esterni non autorizzati	Alto	Possono essere trasferite applicazioni dannose per il PC nella rete informatica	Danneggiamento dei PC o della rete informatica interna
Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari .	Alto	Recupero di dati memorizzati anche dopo la loro cancellazione.	Uso indebito di dati riservati.

Art. 5. Misure di tipo organizzativo

5.1 Assegnazione delle postazioni di lavoro

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a :

- individuare preventivamente le postazioni di lavoro e assegnarle personalmente a ciascun dipendente;
- individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a Internet.

La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

5.2 Nomina dell'Amministratore di sistema

Il datore di lavoro conferisce all'Amministratore di Sistema il compito di sovrintendere alle Risorse Informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:

a. gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'Istituto, siano esse collegate in rete o meno;

b. configurazione dei servizi di accesso alla rete interna, ad Internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account.

c. attivazione della password di accensione (BIOS);

d. creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel Personal Computer che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;

e. controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

f. rimozione, sia sui PC degli incaricati sia sulle unità di rete, di ogni file o applicazione che può essere pericoloso per la Sicurezza o costituisce violazione del presente regolamento;

g. distruzione delle unità di memoria interne alla macchina (hard-disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;

h. utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, ma solo per il tempo strettamente necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al personal computer di ciascuno.

5.3 Utilizzo delle password

5.3.1 Utilizzazione di un sistema di autorizzazione

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'Incaricato della custodia delle Password.

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal custode delle password e consistono in un codice per l'identificazione dell'utente (*user id*), associato ad una parola chiave (*password*) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non può essere divulgata.

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a. la password di accesso al computer impedisce l'utilizzo improprio della postazione, quando per un motivo o per l'altro l'incaricato non si trova in ufficio;
b. la password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
c. la password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato;
d. la password del salvaschermo, infine, impedisce che una assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro dell'incaricato.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).

5.3.2 Procedure di gestione delle credenziali di autenticazione

È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'Amministratore di Sistema a riabilitare l'utente ed assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.

Per scegliere la nuova parola chiave si devono seguire le seguenti istruzioni:

e. usare una parola chiave di almeno otto caratteri;
f. usare una combinazione di caratteri alfabetici e numerici: meglio ancora è inserire almeno un segno di interpunzione o un carattere speciale;
g. non usare mai il proprio nome o cognome, né quello di congiunti (coniuge, figli, genitori), di animali domestici o date di nascita, numeri di telefono etc.. Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe.

La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il Custode delle password. (*L'intervallo raccomandato per il cambio può andare da tre mesi -nel caso di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici- fino a due anni*).

La variazione delle password deve essere comunicata al custode delle password, a cui dovrà essere consegnata in busta chiusa con data e firma dell'incaricato apposte sul lembo di chiusura, perché ne curi la conservazione.

È necessario curare la conservazione della propria parola chiave e bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it, ecc.) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta battendo sulla tastiera quando viene immessa la password.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, all'Amministratore di Sistema dell'Istituto.

Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle Password.

5.4 Utilizzo di internet

La navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. L'accesso a Internet è regolato tramite autenticazione con utente e password, con esclusione dei siti istituzionali.

Il titolare del trattamento provvede alla individuazione delle categorie di siti considerati correlati o non correlati con la prestazione lavorativa

5.5 Utilizzo della posta elettronica

L'istituto mette a disposizione dei lavoratori indirizzi di posta elettronica. Questi possono essere condivisi da due o più lavoratori oppure individuali.

Art. 6. Misure di tipo tecnologico

6.1 Utilizzo della rete informatica

La rete informatica permette di salvare sul server i files relativi alla produttività individuale. Le aree di condivisione in rete sono soggette a regolari attività di controllo, amministrazione e backup. L'accesso è regolato da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

Periodicamente (almeno ogni sei mesi) si provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.

6.2 Utilizzo di internet

L'amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software aventi particolari caratteristiche dimensionali).

6.3 Utilizzo della posta elettronica

Sono previste apposite funzionalità di sistema che consentono:

h. di inviare automaticamente in caso di assenze programmate, messaggi di risposta che contengano le coordinate di un altro soggetto o altri utili modalità di contatto del servizio presso il quale opera il lavoratore assente;

i. al lavoratore, in caso di essenze improvvise o prolungate e per improrogabili necessità legate all'attività lavorativa, di delegare un collega (fiduciario) a verificare il contenuto di messaggi e a inoltrare al responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Art. 7. Diritti e responsabilità dei dipendenti

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità e i lavoratori, garantendo che sia assicurata una ragionevole protezione della loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso di tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo Statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.

Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle Risorse informatiche, dei Servizi e dei programmi ai quali ha accesso e dei dati che tratta.

Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il presente regolamento.

Art. 8. Doveri di comportamento dei dipendenti

Le strumentazioni informatiche, la rete Internet e la posta elettronica devono essere utilizzati dal personale e dagli studenti unicamente come strumenti di lavoro e studio. Ogni loro utilizzo non inerente all'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.

Agli utenti è assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso lingua religione, razza, origine etnica, condizioni di salute, opinioni appartenenza sindacale politica

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

8.1 Utilizzo dei personal computer.

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'istituto, salvo espresse autorizzazioni contrarie dell'Amministratore di sistema/rete, e sono tenuti a:

a. attivare sul PC lo screen saver e la relativa password;
b. conservare la password nella massima riservatezza e con la massima diligenza;
c. non inserire password locali che non rendano accessibile il computer agli amministratori di rete se non esplicitamente autorizzato dall'Amministratore di Sistema;
d. non utilizzare criptosistemi o qualsiasi altro programma di sicurezza crittografia non previste esplicitamente dal servizio informatico dell'istituto;
e. non modificare la configurazione hardware e software del proprio PC, se non esplicitamente autorizzati dall'Amministratore di Sistema;
f. non rimuovere, danneggiare o asportare componenti hardware;
g. non installare sul proprio PC dispositivi hardware personali (modem, schede audio, masterizzatori, pendrive, dischi esterni, i-pod, telefoni, ecc.), salvo specifica autorizzazione in tal senso da parte del responsabile;
h. non installare autonomamente applicazioni o programmi informatici, se non esplicitamente autorizzati dall'Amministratore di Sistema;
i. non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus;
j. mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile;
k. nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica;
l. prestare la massima attenzione ai supporti di origine esterna (es. Pen drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti;
m. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
n. non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet è e ai servizi di posta elettronica;
o. spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

8.2 Utilizzo della rete informatica.

Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente Regolamento e quindi:

a. mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso;
b. provvedere periodicamente (almeno ogni sei mesi) alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante;
c. verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. Pen drive) prima di trasferirlo su aree comuni della rete;

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della Rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di:

a. utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
b. sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate;
c. modificare le configurazioni impostate dall'amministratore di sistema;
d. limitare o negare l'accesso al sistema a utenti legittimi;
e. effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
f. distruggere o alterare dati altrui;
g. usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

8.3 Utilizzo di internet

L'accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. È tassativamente vietato l'utilizzo di modem personali.

Gli utenti sono tenuti a utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente Regolamento e quindi devono:

a. navigare in Internet in siti attinenti allo svolgimento delle mansioni assegnate;
b. registrarsi solo a siti con contenuti legati all'attività lavorativa;
c. partecipare a forum o utilizzare chat solo per motivi strettamente attinenti l'attività lavorativa;

Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'Istituto o a terzi e quindi di:

a. fare conoscere ad altri la password del proprio accesso, inclusi gli amministratori di sistema;
b. usare Internet per motivi personali;
c. servirsi dell'accesso Internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
d. accedere a siti pornografici, di intrattenimento, ecc.;
e. scaricare il software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del responsabile;
f. utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
g. ascoltare la radio o guardare video o filmati utilizzando le risorse Internet;
h. effettuare transazioni finanziarie, operazioni di remote bancking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento;
i. inviare fotografie, dati personali o di amici dalle postazioni Internet.

8.4 Utilizzo della posta elettronica

Gli utenti assegnatari di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti a utilizzarle in modo conforme a quanto stabilito dal presente Regolamento, quindi devono:

a. conservare la password nella massima riservatezza e con la massima diligenza;
b. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
c. utilizzare tecniche per l'invio di comunicazioni a liste di distribuzione solo se istituzionali;

d. inoltrare alla segreteria dell'Istituto ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto e fare riferimento alle procedure in essere per la corrispondenza ordinaria;

e. utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;

f. prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise;

g. inviare preferibilmente file in formato PDF;

h. accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;

i. rispondere a e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;

j. chiamare link contenuti all'interno di messaggi solo quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati;

k. indicare la persona autorizzata ad aprire la posta o la persona che riceverà la posta in caso di assenza.

Agli utenti è fatto espresso divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'Istituto o a terzi e quindi di:

a. prendere visione della posta altrui;

b. simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

c. utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto

d. trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;

e. inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;

f. utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione;

g. inviare o ricevere posta personale attraverso l'uso di un webmail;

h. inviare o accettare messaggi in formato html;

i. utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro.

8.5 Utilizzo dei supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili), per evitare che persone non autorizzate possano accedere ai dati ivi contenuti e quindi in particolare devono:

a. non utilizzare supporti rimovibili personali;

b. custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;

c. consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti all'Amministratore di Sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere, successivamente alla cancellazione, recuperato.

8.6 Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve:

a. applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete;

b. custodirlo con diligenza e in luogo protetto durante gli spostamenti;

c. rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna.

8.7 Utilizzo delle stampanti e dei materiali di consumo

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi o utilizzi eccessivi.

Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati.

Distruggere personalmente e sistematicamente le stampe che non servono più.

8.8 Utilizzo di telefonini e altre apparecchiature di registrazione di immagini e suoni

È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo

- diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;
- informazione preventiva degli interessati;
- acquisizione del loro libero consenso, preventivo ed informato.

Art. 9. Controlli

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi e illeciti può avvalersi legittimamente, nel rispetto dell'articolo 4 comma 2 dello Statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinano il trattamento di dati personali riferibili a singoli utenti.

Il datore di lavoro non può in alcun caso utilizzare detti sistemi per ricostruire l'attività del lavoratore tramite

- lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- memorizzazione sistematica delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite tastiera o dispositivi analoghi;
- analisi occulta dei dispositivi per l'accesso a Internet o alla posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate attraverso il log di sistema ottenuti da un proxy server o da un altro strumento di registrazione delle informazioni. Analogamente sono parimenti suscettibili di controllo i servizi di posta elettronica. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di verifica della funzionalità dei sistemi di protezione e comunque non per più di un anno. Dopo tale periodo, il sistema cancella in modo automatico tali tracciati.

La riservatezza delle informazioni registrate è soggetta a quanto dettato dal D.Lgs. n. 196/2003, il trattamento dei dati avviene esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e in forma anonima in modo tale da precludere l'identificazione degli utenti o delle loro attività. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

- numero di utenti che visita ciascun sito o dominio, numero di pagine richieste e quantità di dati scaricati;
- numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati tassativamente solo nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste dell'autorità giudiziaria e della polizia postale;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiede un immediato intervento;
- in caso di utilizzo anomalo che gli strumenti da parte degli utenti reiterato nonostante l'esplicito invito a ad attenersi a le istruzioni impartite.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'Istituto, il titolare del trattamento procede in forma graduata:

a. in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti;

b. se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, ecc.) o tipologie di utenti (ATA, docenti, studenti) e si procede con avvisi mirati alle categorie di utilizzatori;

c. ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali;

d. in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare

trattamenti in servizio proxy sono curati sono da personale tecnico incaricato del trattamento.

Art. 10. - Informativa agli utenti

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'Istituto e quindi sul sito: www.isamunari.it Esso viene consegnato a ciascun dipendente in forma cartacea assieme all'*informativa ai lavoratori sul trattamento dei dati*.

L'utente, qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prima che questo sia iniziato.

Art. 11. - Sanzioni in caso di mancato rispetto del regolamento

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente:

- può comportare l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti;
- è perseguibile con provvedimenti disciplinari nelle forme con le modalità previste dall'Istituto per gli studenti, dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente;
- può portare alle azioni civili e penali consentite.

L'utilizzo dei servizi di accesso ad Internet cessa o viene sospesa d'ufficio quando:

a. non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso;

b. vi è il sospetto di manomissione dell'hardware o del software;

c. in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc.;

d. in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati;

e. ogni qual volta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

Art. 12. - Aggiornamento e revisione del Regolamento

Il presente Regolamento è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare del trattamento in collaborazione con l'amministratore di sistema.

LICEO ARTISTICO STATALE "BRUNO MUNARI"
VIA GANDHI 14 – 31029 VITTORIO VENETO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

ALLEGATO C

INCARICATI DEL TRATTAMENTO E MANUTENTORI DEL SISTEMA

DICHIARAZIONE AI SENSI DELL'ART. 180, COMMA 2 DEL D.LGS. N. 196/2003

La sottoscritta Dirigente Scolastico del **LICEO ARTISTICO STATALE "BRUNO MUNARI",**

Dichiara

di avere già predisposto ed applicato le misure minime di sicurezza imposte dal D. Lgs. n. 196/2003, Testo Unico in materia di protezione dei dati personali.

Dichiara altresì

che la stessa è da considerarsi come unico "Titolare del trattamento" dei dati personali, sensibili e no, conformemente a quanto stabilito dal D.Lgs. 196/03. Presso la sede amministrativa in via Gandhi n. 14 sono presenti le banche dati e i dati in esse contenuti sono stati forniti dagli utenti, dai dipendenti e dai collaboratori dell'istituzione ai fini dell'adempimento di obblighi istituzionali e/o amministrativo-contabili.
I codici utilizzati sono quelli di cui all'allegato della Notifica al Garante.

Firma del titolare del trattamento _____

Il LICEO ARTISTICO STATALE - "BRUNO MUNARI",

nella persona del Dirigente Scolastico, titolare del trattamento dei dati personali, considerato quanto previsto dal manuale della privacy nomina membri della conferenza dei responsabili i seguenti soggetti:

DSGA – *Sig.ra Lucia Magnano*

Collaboratori del Dirigente Scolastico – *Prof.Francesco Puliatti*

F.S. area 1 – *Prof.ssa Gianna Miglietta*

F.S. area 2 e area 6 – *Prof. Maurizio Armellin*

F.S. area 11 – *Profssa Anna Giacobbi e Prof.ssa Paola Alessandra Vacalebre*

F.S. area 15 – *Prof. L. Pincin*

presidente della Conferenza è il Titolare del Trattamento nella persona del Dirigente Scolastico.

Compiti della Conferenza dei Responsabili:

1. verifica la modulistica predisposta e le istruzioni da fornire agli incaricati del trattamento;
2. valuta le attività del trattamento svolte da soggetti esterni all'istituto scolastico a tal fine nominati responsabili o incaricati;
3. discute il programma per la sicurezza del trattamento dei dati scolastici e si confronta sulle risorse economiche e umane da utilizzare;
4. verifica le modifiche da apportare al manuale e propone la revisione annuale;
5. verifica i risultati degli audit svolti;
6. controlla le richieste di accesso da parte degli interessati e il soddisfacimento dei diritti previsti dall'art. 7 del D.Lgs. n.196/2003;
7. relaziona annualmente sulle attività di trattamento;
8. programma l'attività di vigilanza come predisposto dalla sezione 06 punto 6.4.1 del manuale;
9. conserva il manuale e ne verifica la corretta applicazione;
10. stabilisce la distribuzione del manuale a tutti coloro che trattano i dati per conto dell'Istituto.

IL TITOLARE DEL TRATTAMENTO

Per accettazione

I SOGGETTI NOMINATI

Lista degli incaricati del trattamento e dei manutentori del sistema

All.B D.Lgs. 196/03

Estremi dei provvedimenti adottati

Data Provvedimento	Tipo Provvedimento	Oggetto	Soggetti autorizzati	Banca dati del trattamento
Prot. N. 4822 Data 07/09/2009	Lettera di incarico del Titolare	Nomina del Responsabile al trattamento di dati personali	Dsga Lucia Magnano	Personale ata, docente
Prot. N. 6968 Data 15.12.2010	Lettera di incarico del Titolare	Incarico di Amministratore di Sistema	Assistente tecnico Marta Colapietro	Personale ata, docente
Prot. N. 1581 Data 19/03/2010	Lettera di incarico del Titolare	Incarico di Gestore della Rete informatica	Ditta ETRE di Villorba	database
Prot. N. 1581 Data 19/03/2010	Lettera di incarico del Titolare	Incarico di Responsabile esterno della Rete informatica per il SIDI	Ditta Argo Software di Ragusa	Graduatorie ATA e docenti
Prot. N. 4822 Data 07/09/2009	Lettera di incarico del Titolare	Incarico di custode delle password	Assistente amm.va Mariella Dal Pio Luogo	
Prot. N. 4822 Data 07/09/2009	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (assistenti amministrativi)	Mariella Dal Pio Luogo Giannina Tonon Sandra Zandonà	Protocollo Personale Alunni
Prot. N. 4518 Data 03/09/2010	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (assistenti amministrativi)	Milena Ulian Paloa Zaccaron Luisa Paris	Contabilità Magazzino
Prot. N. 4822 Data 07/09/2009	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (docenti)	Docenti	Personale docente

Prot. N. 4517 Data 03/09/2010	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (docenti)	Docenti	Personale docente
Prot. N. 1775 Data 30/03/2011	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (docenti)	Docenti	Personale docente
Prot. N. 4822 Data 07/09/2009	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (Collaboratori Scolastici)	Collaboratori scolastici	Personale collaboratore scolastico
Prot. N. 4519 Data 03/09/2010	Nomina del Responsabile al Trattamento	Individuazione degli incaricati al trattamento di dati personali da parte (Collaboratori Scolastici)	Collaboratori scolastici	Personale collaboratore scolastico

Lettera di incarico al Responsabile del Trattamento

Art. 29 D.Lgs. 196/03

In qualità di "Titolare del Trattamento" dei dati personali, conformemente a quanto stabilito dal D.Lgs. n. 196 del 30/06/2003, il Liceo Artistico Statale "Bruno Munari" di Vittorio Veneto, nella persona del dirigente scolastico in qualità di legale rappresentante, previa verifica dell'esperienza, capacità, affidabilità in ordine alle garanzie volte al rispetto della sicurezza del trattamento dei dati personali,

AFFIDA

alla sig.ra …… l'incarico di **Responsabile del Trattamento** per le banche dati di cui a seguire si riportano le indicazioni relative alla natura e ai luoghi di residenza dei dati, alle finalità e modalità del trattamento autorizzate nonché alle tipologie di comunicazione e diffusione ammesse.

Si ricorda che costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o telematici, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Il Responsabile del Trattamento ha il compito di curare lo svolgimento del trattamento di dati, per quanto di propria competenza, e provvedere a:

- collaborare col Titolare nella predisposizione del Documento Programmatico sulla Sicurezza e degli altri documenti necessari in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e ciò al fine di custodire e controllare i dati. L'adeguatezza delle misure deve essere valutata in relazione alle conoscenze relative al progresso tecnico, alla natura dei dati trattati e alle specifiche caratteristiche del trattamento;
- informare il Titolare nella eventualità che si siano rilevati dei rischi e segnalare le misure di sicurezza idonee e preventive da adottare ai sensi degli articoli da 33 a 36 del D.Lgs. n.196/2003 e del disciplinare tecnico di cui all'allegato B del medesimo;
- adottare le misure di sicurezza minime ai sensi degli articoli da 33 a 36 del Testo Unico in materia tenendo conto che le misure di protezione sono individuate dal disciplinare tecnico allegato B del Testo Unico e differenziate a seconda degli strumenti utilizzati per il trattamento (automatizzati oppure no) e della natura dei dati trattati (sensibili, giudiziari, comuni);
- individuare, nominare e incaricare per iscritto, un "Custode delle Password" e l'"Amministratore di Sistema";
- organizzare gli archivi cartacei in modo da garantire adeguata protezione dei dati, anche in relazione al loro grado di sensibilità e di delicatezza, nonché la protezione da eventi che potrebbero danneggiare o far perdere documenti;
- redigere ed aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione connessi in rete, nonché l'elenco delle tipologie dei trattamenti effettuati;
- comunicare all'Amministratore di sistema ogni variazione di contesto rispetto alla situazione esistente, in particolare ogni modifica del software applicativo (programmi gestionali) o del software di produttività individuale (office, etc) e di ogni altro componente presente o di nuova implementazione;
- individuare e incaricare per iscritto gli Incaricati del trattamento, delineandone i profili e impartendo loro in forma scritta le istruzioni necessarie per un corretto, lecito e sicuro trattamento nonché adeguate prescrizioni sulle misure di sicurezza da applicare. Si precisa che devono essere individuati e incaricati tutti i soggetti che, a vario titolo, svolgono operazioni di trattamento di dati, per finalità e per conto dell'Istituto Scolastico Titolare, anche se temporaneamente;
- autorizzare i singoli incaricati del trattamento e della manutenzione di dati sensibili e giudiziari, applicando le autorizzazioni previste da espressa disposizione di legge o provvedimento del Garante;
- organizzare la formazione per gli incaricati;

- procedere alle verifiche sulla qualità, la pertinenza, non eccedenza e completezza dei dati trattati, verificare la corrispondenza delle finalità del trattamento rispetto alle disposizioni di legge e soprattutto al consenso manifestato dall'interessato nel caso di trattamento di dati sensibili,
- controllare l'esattezza e la conformità dei dati tra il momento della raccolta e quello del loro successivo utilizzo e provvedere al loro aggiornamento in caso di riscontrate variazioni;
- disporre il blocco dei dati qualora si renda necessaria la sospensione temporanea e disporne inoltre la loro cancellazione qualora necessaria;
- procedere periodicamente alle verifiche sulla metodologia di raccolta e gestione dei dati e garantire che tutte le misure di sicurezza riguardanti i dati detenuti dall'Istituto siano applicate;
- definire le modalità di accesso ai locali;
- attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- rispondere tempestivamente alle richieste ed eventuali reclami degli interessati, tenendo presente che l'interessato al trattamento dei dati personali può esercitare il diritto di accesso alle proprie informazioni ed inoltre che può chiedere l'aggiornamento, la rettifica e, qualora vi abbia interesse, l'integrazione dei dati ed anche la cancellazione o la trasformazione dei dati in forma anonima;
- interagire con soggetti che per legge compiono verifiche, controlli o ispezioni sugli adempimenti della privacy.

Il Responsabile del Trattamento nello svolgere i compiti assegnati deve:

- agire in modo lecito e secondo correttezza;
- raccogliere e trattare i dati esclusivamente per le finalità e gli scopi dell'Istituto;
- verificare che i dati siano esatti, pertinenti e non eccedenti le finalità per cui sono stati raccolti e trattati. e provvedere al loro aggiornamento.

Si ricorda che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

Vittorio Veneto lì ……

Il Titolare del Trattamento ……

La Sig.ra ……

accetta la nomina di Responsabile del Trattamento dei dati personali e:

- dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. n. 196 del 30/06/2003,
- impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte,
- si impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare.

Il Responsabile del Trattamento per accettazione ……

Incarico Amministratore di sistema

La sottoscritta Prof.ssa Franca Braido, in qualità di rappresentante legale del Liceo Artistico Statale "Bruno Munari" e Titolare del trattamento dei dati ai sensi del D.lgs N. 196 del 30/06/2003,

- visto il decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e l'allegato tecnico al codice sulla privacy e sue successive modifiche ed aggiornamenti che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- considerato che l'incarico in oggetto attiene a fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati;
- verificate le competenze della persona a cui è assegnato il presente incarico e, per quanto ragionevolmente possibile, la sua idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni in materia di sicurezza del trattamento dei dati;
- verificata la disponibilità di personale interno all'Istituzione scolastica per l'incarico in oggetto

oppure

- constatata l'impossibilità di ricorrere a competenze interne nelle materie in oggetto;
- verificate le procedure di scelta del contraente inserite nel regolamento di istituto,

in base al vigente disciplinare e fatte salve le successive integrazioni dello stesso

affida alla Sig.ra …… l'incarico di Amministratore di sistema

con i compiti sotto riportati, per garantire che i dati personali contenuti nei vari archivi informatici siano custoditi e controllati al fine di ridurre al minimo i rischi di:

- distruzione o perdita anche accidentale dei dati stessi;
- accesso non autorizzato;
- trattamento non consentito, o non conforme alle finalità della raccolta.

In relazione a tale incarico, la Sig.ra …… ha il compito di sovrintendere alle risorse del sistema informativo dell'Istituto ed, in particolare, attenendosi alle disposizioni del Titolare del trattamento e collaborando con il Responsabile del trattamento (*se nominato*), deve progettare, realizzare e mantenere in efficienza misure di sicurezza tali, da soddisfare le linee strategiche di indirizzo definite dal titolare e quindi:

- cooperare nella predisposizione ed aggiornamento annuale del documento programmatico sulla sicurezza per la parte concernente il sistema informatico ed il trattamento informatico dei dati e quindi:
  - definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi, delle procedure e dei sistemi informatici esistenti
  - definire un'architettura di sicurezza, che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione, e provvedere all'aggiornamento periodico del sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce;
  - realizzare la progettazione esecutiva del sistema di sicurezza, con particolare riferimento alla identificazione degli elementi da proteggere
- emanare procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, le operazioni giornaliere di sicurezza dei dati e dei sistemi, ecc.
- sovrintendere al funzionamento della rete e monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica, per assicurarne costante efficienza e disponibilità;

- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- aggiornare periodicamente, con frequenza almeno annuale (*oppure* semestrale *se si trattano dati sensibili o giudiziari*), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti (firewall, filtri per la posta elettronica, antivirus, ecc);
- predisporre ed implementare le ulteriori misure minime di sicurezza imposte dal disciplinare per il trattamento informatico dei dati sensibili e giudiziari e per la conseguente tutela degli strumenti elettronici
    - verificare, con cadenza almeno annuale (*oppure* semestrale *se si trattano dati sensibili*) l'installazione, l'aggiornamento ed il funzionamento di idonei strumenti elettronici atti a proteggere contro il rischio di intrusione i dati *sensibili o giudiziari* trattati attraverso gli elaboratori;
    - impartire istruzioni organizzative e tecniche per la custodia, l'uso, il riutilizzo o la distruzione dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
    - consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
- predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema stesso, avendo cura che tali registrazioni (access log) abbiano caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
- assistere il Titolare (o, *se nominato,* il Responsabile del trattamento) nell'impostazione e gestione operativa del sistema di attribuzione dei codici di accesso agli strumenti informatici e di autorizzazione al trattamento di dati personali, conforme a quanto previsto dai punti da 1 a 10 e dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda finalizzate all'accesso al sistema informativo, collaborando con il custode delle password (*se nominato*) e vigilando sulla sua attività (*oppure svolgendo anche la funzione di custode delle copie delle credenziali*);
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni e impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda
- verificare costantemente che l'Istituto abbia adottato le misure minime di sicurezza per il trattamento dei dati personali provvedendo in collaborazione con il Responsabile del trattamento dei dati personali (*se nominato*) agli aggiornamenti eventualmente necessari anche per adeguare il sistema ad eventuali nuove norme in materia di sicurezza;
- verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore e quindi che il software utilizzato sia originale licenziato e in caso di applicazioni gestionali, siano garantite le corrette installazioni delle releases rilasciate;
- fornire supporto alla formazione del personale dell'organizzazione, in tema di sicurezza.

In relazione ai compiti affidati l'Amministratore di sistema s'impegna ad adottare tutte le misure necessarie all'attuazione di quanto descritto nel Documento Programmatico sulla Sicurezza di questo Istituto.

L'Amministratore testé incaricato si impegna a riferire periodicamente, ed in ogni caso con cadenza semestrale, al Titolare del trattamento sullo svolgimento dei suoi compiti, e ad informare il Responsabile del trattamento o il Titolare di qualsiasi situazione che possa compromettere il corretto trattamento informatico dei dati personali, anche a causa del mancato rispetto delle norme di sicurezza o eventuali incidenti occorsi.

IL TITOLARE DEL TRATTAMENTO ……

La Sig.ra …….……..……..

accetta la nomina di Amministrazione di sistema

e dichiara di essere a conoscenza:

1. di quanto stabilito dal D.lgs n. 196 del 30/06/2003 e di fornire garanzia del pieno rispetto delle

vigenti disposizioni in materia di trattamento e delle prescrizioni impartite dal Titolare dei dati, ivi compreso il profilo relativo alla loro sicurezza ed in particolare:

a. di conoscere e impegnarsi a rispettare, sotto la propria responsabilità e nell'ambito delle materie oggetto del presente incarico, quanto indicato nell'allegato B del "Disciplinare tecnico in materia di misure minime di sicurezza";
b. di attenersi agli obblighi di assoluta riservatezza connessi al suo incarico e pertanto si impegna a rispettare il divieto assoluto di comunicare e diffondere, nel corso e alla cessazione dell'incarico stesso senza limiti temporali, a terzi non autorizzati le informazioni e i dati personali di cui sia venuto a conoscenza; impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare
c. di trattare dati personali solo se ciò è indispensabile in relazione all'assolvimento degli incarichi assegnati;

2. che qualora la sua attività riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, sarà resa conoscibile l'identità dell'Amministratore di sistema nell'ambito dell'organizzazione;
3. che il suo l'operato sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare o del Responsabili 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.

La sig.ra ……..…..…… per accettazione dell'incarico ……..

……

Lettera di incarico al Custode delle password

(Disciplinare tecnico allegato al D.Lgs. 196/03)

In qualità di "Titolare del Trattamento" dei dati personali, conformemente a quanto stabilito dal D.Lgs. n. 196 del 30/06/2003, il Liceo Artistico Statale "Bruno Munari" di Vittorio Veneto, nella persona del dirigente scolastico in qualità di legale rappresentante, previa verifica dell'esperienza, capacità, affidabilità in ordine alle garanzie volte al rispetto della sicurezza del trattamento dei dati personali,

AFFIDA

alla sig.ra …… l'incarico di Custode delle password attribuite ai singoli incaricati al trattamento dei dati con strumenti elettronici in Istituto come imposto dal Disciplinare tecnico allegato al D.Lgs. 196/03.

Nell'espletamento delle sue funzioni il Custode delle password dovrà applicare le misure di sicurezza disposte dall'Istituto e, specificatamente, nelle gestione delle parole chiave dovrà:

- collaborare con il responsabile del trattamento per la corretta gestione delle misure di sicurezza relative alle parole chiave;
- gestire il sistema delle parole chiave con modalità, fisiche ed organizzative, atte a garantire la segretezza delle stesse e la loro integrità;
- ricevere dai singoli incaricati del trattamento comunicazione riservata della sostituzione di password effettuata;
- intervenire sul profilo autorizzativo del singolo incaricato per permettere all'Istituto, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dallo stesso, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività in caso di prolungata assenza od impedimento dell'incaricato, che renda indispensabile ed indifferibile l'intervento, informando tempestivamente l'incaricato dell'accesso realizzato.

Si ricorda che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

Vittorio Veneto lì ……..

Il Titolare del Trattamento ……

La Sig.ra ……..

accetta la nomina di Custode delle password e:

- dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. n. 196 del 30/06/2003 e del Disciplinare tecnico allegato,
- si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte,
- si impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare.

Il Custode delle password per accettazione ……

Nomina degli assistenti amministrativi in qualità di incaricati del trattamento dei dati personali

Ai sensi del D.Lgs 30.6.2003 n.196 che regolamenta il trattamento dei dati personali e disciplina la gestione delle banche dati utilizzate, con il presente atto il Responsabile del Trattamento del Liceo Artistico Statale "Bruno Munari" di Vittorio Veneto

INCARICA

la Sig.ra …… di svolgere operazioni di trattamento dei dati personali degli alunni finalizzate alla gestione delle banche dati "……." cartacee ed informatiche, di cui a seguire si riportano le indicazioni relative alla natura e ai luoghi di residenza dei dati, alle finalità e modalità del trattamento autorizzate nonché alle tipologie di comunicazione e diffusione ammesse.

Si ricorda che costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Con il presente incarico e per la banca dati indicata la sig.ra ……. è autorizzata alle operazioni di inserimento – modifica – rimozione – visualizzazione e stampa di dati personali, sensibili e giudiziari degli alunni pertinenti, completi e non eccedenti rispetto alle finalità per cui si agisce e in conformità alle informazioni che l'Istituto ha comunicato agli interessati.

L'incaricato/a, nello svolgere le operazioni, deve:

- agire in modo lecito e secondo correttezza;
- raccogliere e trattare i dati esclusivamente per le finalità specificate nell'allegato "Banca dati ……" (costituente parte integrante delle istruzioni in oggetto), in relazione al proprio profilo di appartenenza;
- verificare che i dati siano esatti e provvedere al loro aggiornamento.

Inoltre l'incaricato deve:

- ai sensi dell'art. 13 del D.Lgs. n. 196/03 non procedere alla raccolta e al trattamento dei dati se non è stata fornita previamente l'informativa all'interessato o alla persona presso cui si raccolgono i dati;
- acquisire, nei casi non di esonero e per il trattamento di dati sensibili, il modulo per il consenso opportunamente firmato da parte dell'interessato o di chi lo rappresenti;
- rispettare le misure di protezione e sicurezza necessarie ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito adottate dal Titolare e dal Responsabile, ed atte a salvaguardare la riservatezza e l'integrità dei dati, riportate in allegato e quelle specificate dal Disciplinare nonché a quelle che dovessero successivamente essere comunicate;
- informare prontamente il Responsabile del Trattamento di tutte le questioni rilevanti ai fini di legge in materia di trattamento di dati personali;

Si ricorda che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

Vittorio Veneto lì ……..……

Il Responsabile del Trattamento ….……

L'incaricato/a del trattamento dei dati:

- è a conoscenza che deve operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) ed elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite;
- si impegna a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 Del D.Lgs. n.196/2003; in particolare sapendo che i dati devono essere trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi; i dati devono

essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

- dichiara di avere ricevuto, esaminato e compreso le linee guida in materia di sicurezza;
- si impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare.

L'incaricato del trattamento per accettazione ……

Nomina dei docenti in qualità di incaricati del trattamento dei dati personali

Ai sensi del D.Lgs 30.6.2003 n.196 che regolamenta il trattamento dei dati personali e disciplina la gestione delle banche dati utilizzate, con il presente atto il Responsabile del Trattamento del Liceo Artistico Statale "Bruno Munari" di Vittorio Veneto

INCARICA

Il/la Prof. …… di svolgere operazioni di trattamento dei dati personali degli alunni finalizzate all'espletamento dei compiti propri del profilo professionale, di cui a seguire si riportano le indicazioni relative alla natura e ai luoghi di residenza dei dati, alle finalità e modalità del trattamento autorizzate nonché alle tipologie di comunicazione e diffusione ammesse.

Si ricorda che costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati. I dati trattati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per cui si agisce.

L'incaricato/a, nello svolgere le operazioni, deve:

- agire in modo lecito e secondo correttezza;
- raccogliere e trattare esclusivamente i dati ammessi e per le finalità specificate nella scheda di istruzioni operative in relazione al profilo di appartenenza;
- verificare che i dati siano esatti e provvedere al loro aggiornamento.

Inoltre l'incaricato/a deve:

- ai sensi dell'art. 13 del D.Lgs. n. 196/2003 non procedere alla raccolta e al trattamento dei dati senza che sia stata fornita previamente, utilizzando gli appositi moduli, l'informativa all'interessato o alla persona presso cui si raccolgono i dati;
- acquisire, nei casi non di esonero e per il trattamento di dati sensibili, il modulo per il consenso opportunamente firmato da parte dell'interessato o di chi lo rappresenti;
- rispettare le misure di sicurezza minime e idonee adottate dal Titolare e dal Responsabile, atte a salvaguardare la riservatezza e l'integrità dei dati previste dalla scheda di istruzioni operative;
- informare prontamente il Responsabile del Trattamento di tutte le questioni rilevanti ai sensi del Testo Unico in materia di trattamento di dati personali;
- comunicare tempestivamente e per iscritto al Dirigente Scolastico eventuali smarrimenti e/o alterazioni dei Registri e/o dei dati personali riguardanti gli alunni.

Si ricorda che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dal Responsabile, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

Vittorio Veneto lì ……

Il Responsabile del Trattamento ……..……

L'incaricato/a del trattamento dei dati:

- è a conoscenza che deve operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) ed elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite;
- si impegna a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 del D.Lgs. n.196/2003; in particolare sapendo che i dati devono essere trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi; i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- dichiara di avere ricevuto, esaminato e compreso le linee guida predisposte per i docenti in materia di sicurezza;
- si impegna a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza,

- si impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare.

L'incaricato del trattamento per accettazione ……

Nomina dei collaboratori scolastici nella qualità di incaricati del trattamento dei dati personali

Ai sensi del D.Lgs 30.6.2003 n.196 che regolamenta il trattamento dei dati personali e disciplina la gestione delle banche dati utilizzate, con il presente atto il Responsabile del Trattamento del Liceo Artistico Statale "Bruno Munari" di Vittorio Veneto

INCARICA

Il/la Sig./Sig.ra …… di svolgere operazioni di trattamento dei dati personali nell'ambito dei compiti di collaborazione con l'ufficio di segreteria previsti dal piano annuale dei servizi amministrativi e generali. Si ricorda che:

- costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati;
- l'incaricato/a nello svolgere le operazioni di gestione delle comunicazioni telefoniche e a mezzo fax, duplicazione attraverso fotocopie, trasporto documenti e posta e trasferimento tra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali nonché collaborazione nelle operazioni di archiviazione, scarto ed eliminazione di documenti deve agire:
  - in modo lecito e secondo correttezza;
  - seguire le misure di sicurezza adottate dal Titolare e dal Responsabile del trattamento, atte a salvaguardare la riservatezza e l'integrità dei dati e previste dalla scheda di istruzioni;
  - informare prontamente il Responsabile del Trattamento di tutte le questioni rilevanti ai sensi del Testo Unico in materia di trattamento di dati personali;

Si ricorda che in base alla legge sulla privacy il Titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003, in materia di sicurezza. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

Vittorio Veneto lì ……..…..……

Il Responsabile del Trattamento ….……..……

L'incaricato/a del trattamento dei dati:

- è a conoscenza che deve operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) ed elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite;
- si impegna a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 del D.Lgs. n.196/2003; in particolare sapendo che i dati devono essere trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi; i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- dichiara di avere ricevuto, esaminato e compreso le linee guida in materia di sicurezza;
- si impegna, nel corso del presente incarico e alla cessazione dello stesso senza limiti temporali, a rispettare il divieto di comunicazione e diffusione ad altri e a qualunque titolo dei dati trattati e di qualsiasi tipo di informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Titolare.

L'incaricato del trattamento per accettazione ….……

LICEO ARTISTICO STATALE "BRUNO MUNARI"
VIA GANDHI 14 – 31029 VITTORIO VENETO

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

ALLEGATO D

TUTELA DIRITTI DELL'INTERESSATO

1. **Informativa**
2. **Procedura di accesso**

Firma del Titolare del Trattamento _____

Informativa sul trattamento dei dati personali e sensibili

Art. 13 D. Lgs 196/03

Desidero informarLa che il Codice in materia di protezione dei dati personali prevede che il loro trattamento sia improntato ai principi di correttezza, liceità e trasparenza, nonché di tutela della Sua riservatezza e dei Suoi diritti.

Per garantire la tutela della riservatezza dei propri utenti e per prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, questo Istituto ha predisposto un manuale in cui sono descritti gli adempimenti necessari e riportate le istruzioni impartite ai propri operatori.

Il manuale, in visione presso la segreteria, prevede che Le vengano fornite le informazioni, riportate in questo opuscolo, perché Lei possa conoscere le modalità del trattamento dei dati che la riguardano.

Il Dirigente Scolastico

Oggetto e finalità del trattamento

I dati personali riguardanti l'alunno o i suoi familiari sono raccolti e trattati da questo Istituto per l'esclusivo assolvimento degli obblighi istituzionali della scuola, quindi riguardanti l'istruzione e la formazione degli studenti, e per le finalità amministrative strettamente connesse e strumentali alla gestione dei rapporti con gli alunni stessi nonché agli obblighi previsti da leggi e regolamenti in materia di istruzione ed assistenza scolastica.

Il trattamento riguarda anche eventuali dati personali rientranti nel novero dei dati *sensibili*, vale a dire dati "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". A questi si aggiungono i dati giudiziari, cioè informazioni riguardanti procedimenti o provvedimenti di natura giudiziaria. Tutti questi dati saranno trattati dalla scuola secondo quanto previsto dalle disposizioni di legge in modo da tutelare il diritto alla riservatezza, non ledere la sensibilità, limitare la libertà o determinare alcuna discriminazione.

Consenso al trattamento e conseguenze dell'eventuale rifiuto

Il conferimento dei dati personali richiesti è obbligatorio poiché necessario alla realizzazione delle finalità istituzionali e l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione, ad esempio per l'assegnazione del docente di sostegno, l'esonero da alcune attività didattiche, l'idoneità all'attività di laboratorio, l'inserimento di alunni stranieri, ecc.

Modalità del trattamento

In relazione alle finalità indicate, il trattamento dei dati personali verrà effettuato sia in forma cartacea che con strumenti informatici.

I dati saranno trattati esclusivamente dai soggetti autorizzati e in modo da garantire la massima sicurezza. Nel caso di dati *sensibili*, il trattamento viene effettuato con l'attenzione e la cautela previste dalle disposizioni di legge e dai Regolamenti emanati dal Ministero, in particolare essi non possono essere mai oggetto di diffusione.

Soggetti a cui potranno essere comunicati i dati personali

I dati personali, diversi da quelli sensibili e giudiziari, potranno essere comunicati esclusivamente a soggetti pubblici, se previsto da disposizioni di legge o regolamento.

Tali dati possono essere comunicati, per fini istituzionali e previa autorizzazione dell'interessato, ad alcune categorie di soggetti privati, quali ad esempio:

soggetti privati, al solo fine di agevolare, per gli studenti di scuola secondaria, l'orientamento, la formazione, l'esperienza di stage o alternanza scuola/lavoro e/o l'inserimento professionale degli alunni, limitatamente ai dati personali o relativi agli esiti scolastici, comunque diversi da quelli sensibili o giudiziari, e fatta salva la tutela della riservatezza dell'alunno e la sua possibilità di opporsi alla loro comunicazione;

altri soggetti su richiesta degli interessati.

Al momento dell'iscrizione le verrà fornito l'apposito modulo per dichiarare o meno il suo consenso all'utilizzo dei dati per queste finalità.

I dati relativi agli esiti scolastici degli alunni vengono pubblicati mediante affissione all'albo nei termini previsti dalle vigenti disposizioni in materia.

Diritti dell'interessato

In ogni momento Lei potrà esercitare i Suoi diritti nei confronti del titolare del trattamento dei dati, ai sensi dell'art.7 del D.lgs.196/2003, 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 venirne 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, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali sono 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 rileva 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.*

Per esercitare tali diritti Lei può presentare istanza alla segreteria dell'Istituto, che Le fornirà l'apposito modulo.

Il titolare del trattamento dei dati è **i**l Liceo Artistico Statale "Bruno Munari"

Il rappresentante pro tempore del titolare nel territorio dello Stato è il Dirigente Scolastico.

Il responsabile del trattamento è la sig.ra Lucia Magnano

Recapito: Via Gandhi 14 - 31029 Vittorio Veneto

e-mail isamunari@isamunari.it sito internet www.isamunari.it

Dichiaro di aver ricevuto l'informativa di cui all'art. 13 del D.Lgs. n. 196/2003.

Data, ...

.....

PROCEDURA PER LA GESTIONE DEL DIRITTO DI ACCESSO DELL'INTERESSATO

ex art. 7 D.Lgs. n. 196/2003 (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 venirne 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, l'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 e' 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

Per favorire l'esercizio dei diritti dell'interessato in modo tempestivo e nell'ottica del maggior rispetto dei diritti soggettivi del medesimo è adottata la seguente procedura per la gestione del diritto di accesso:

1. Gli interessati devono presentare le loro richieste al responsabile del trattamento
   - oralmente, in tal caso vanno registrate a cura del responsabile o del suo incaricato
   - in forma scritta mediante l'apposito modulo prestampato (MAS 04.10) ovvero a mezzo posta, per fax e per posta elettronica se con firma digitale. Non è necessario che l'interessato presenti le proprie motivazioni tranne che quando la motivazione riguardi l'opposizione per motivi legittimi.
2. La richiesta può provenire anche da una persona fisica diversa dall'interessato o da un'associazione purché provvista di delega dell'interessato stesso. In tal caso l'ufficio deve chiedere l'esibizione della procura o delega unitamente a copia fotostatica non autenticata di un documento di identificazione.
3. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

   Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
4. La risposta del responsabile del trattamento alle richieste avanzate deve essere spedita o consegnata non oltre il termine di 30 giorni dal deposito dell'istanza.

Il Titolare del Trattamento

MODULO PER LA RICHIESTA DI ACCESSO AL TRATTAMENTO

Il sottoscritto ……., nato a …… il ……., residente in ……..……ai sensi dell'art. 7 del Testo Unico in materia di trattamento di dati personali di cui al Decreto Legislativo 30 giugno 2003 n. 196,

chiede

di essere informato sull'identità dei responsabili e sulle finalità e modalità del trattamento svolto da codesto Istituto Scolastico

chiede inoltre di ottenere

senza ritardo (barrare la casella che interessa)

I seguenti dati che lo riguardano:

……
……
……

- ❑ la conferma dell'esistenza o meno di dati che lo riguardano
- ❑ la cancellazione dei dati perché trattati in violazione dell'art. ……
- ❑ la trasformazione in forma anonima perché in violazione legge ……
- ❑ il blocco dei dati per violazione delle disposizioni ……
- ❑ l'aggiornamento ……
- ❑ la rettificazione ……
- ❑ l'integrazione ……

Dichiara di opporsi al trattamento dei dati che lo riguardano per i seguenti motivi

……
……
……

Luogo e data …… Firma Interessato ……

LICEO ARTISTICO STATALE - "BRUNO MUNARI"
VIA GANDHI 14 - 31029 VITTORIO VENETO (TV)

REGISTRI

1. Registro carico/scarico documenti sensibili
2. Registro annuale virus
3. Registro annuale rischio hardware
4. Registro annuale rischio applicazione
5. Registro annuale rischio sistema operativo
6. Registro annuale rischio luoghi dove vengono trattati i dati
7. Documento di verifica del rispetto degli adempimenti richiesti e dell'attività dell'amministratore di sistema

Firma del Titolare del Trattamento _____

LICEO ARTISTICO STATALE - "BRUNO MUNARI" VIA GANDHI 14 VITTORIO VENETO 31029 TV	Manuale della Privacy	04.06 rev. del 30/03/2011
	Registro carico/scarico documentazione sensibile	

Data Richiesta	Richiedente		Modalità Richiesta	Finalità Richiesta	Visione	copia	Data Comunicazione	Sigla Incaricato
	Cognome	Nome						
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		

			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		
			□ Orale □ Fax □ Telefonicamente □ Spedito per posta o corriere □ Consegnato a mano		□ □ □ □ □	□ □ □ □ □		

LICEO ARTISTICO STATALE - "BRUNO MUNARI" VIA GANDHI 14 VITTORIO VENETO 31029 TV	Manuale della Privacy	04.12 rev. del 30/03/2011
	REPORT ANNUALE VIRUS	

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
97520375 didattica	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
16870192 protocollo	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
10558324 magazzino	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
X13-04660 segreteria-ufficio tecnico	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
97 52 0382 personale	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
YLJ073574 contabilità	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
CZC74039K3 dsga	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
W88487B81G0 mac portatile	Intel Core I7	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
X1060256 vice presidenza	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
0045-619790-743 funzione strumentale	Intel Pentium IV	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore	Tipo di Antivirus Utilizzato	Periodicità di aggiornamento
01110038520 presidenza	Amd Turion II Dual-Core M500	Antivirus F-SECURE e Watchguard Firewall Firebox X550E	Ogni 6 mesi

Data	Tipo di virus rilevato	Provenienza	Danno scarso	Danno medio	Danno alto	Danno nessuno	Azione correttiva	Firma del R.D.T.

LICEO ARTISTICO STATALE - "BRUNO MUNARI" VIA GANDHI 14 VITTORIO VENETO 31029 TV	Manuale della Privacy	04.13
	REPORT ANNUALE RISCHI HARDWARE	rev. del 30/03/2011

Sistema di Elaborazione	Tipo di Elaboratore
97520375 didattica	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
16870792 protocollo	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
10558324 magazzino	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
X13-04660 segreteria – ufficio tecnico	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
YLJ073574 personale	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
X10-37254 contabilità	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
CZC74039K3 dsga	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
W88487B81G0 mac portatile	Intel Core I7

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
X1060256 vice presidenza	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
0045-619790-743 funzione strumentale	Intel Pentium IV

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sistema di Elaborazione	Tipo di Elaboratore
01110038520 presidenza	Amd Turion II Dual-Core M500

Data	Tipo di rischio rilevato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

LICEO ARTISTICO STATALE - "BRUNO MUNARI" VIA GANDHI 14 VITTORIO VENETO 31029 TV	Manuale della Privacy REPORT ANNUALE RISCHIO APPLICAZIONE	04.14 rev. del 30/03/2011

Applicazione	Descrizione
Antivirus F-SECURE business suite educational	licenza antivirus per n. 10 personal computer per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Kit Scuola Std OLP NL W32 IT (OfficStdFPage2000/VBStd6/Crt Wrt Bundle)	Licenza microsoft per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Microsoft Office Professional 2000 Win32 Italian Academic OPEN	Licenza Office per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Microsoft Publisher 2000 Win32 Italian Academic OPEN No Level	licenza Office per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Libri di testo win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Fisco win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Alunni win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Scrutinio win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Personale win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Sybase SQL Anywhere Studio	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Protocollo win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Bilancio win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Emolumenti win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Inventario win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Magazzino win	licenza d'uso Argo per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Microsoft Office XP Professional Win32 Italian Academic OPEN No Level	licenza microsoft Office

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Descrizione
Microsoft Office Professional 2003 Win32 Italian Academic OPEN No Level	licenza Office per segreteria

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Windows Svr Std 2003 Win32 Italian OLP NL AE	2003

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Windows Server CAL 2003 Italian OLP NL AE Device CAL	2003

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Microsoft Open License	2005

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Microsoft Office Professional 2003 Win32 Italian Academic OPEN No Level	2005

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Microsoft Windows 2000 Server Italian	2000

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Applicazione	Versione
Microsoft Windows 2000 Server CAL Italian	2000

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

LICEO ARTISTICO STATALE - "BRUNO MUNARI" VIA GANDHI 14 VITTORIO VENETO 31029 TV	Manuale della Privacy	04.16
	REPORT ANNUALE RISCHI LUOGHI OVE VENGONO TRATTATI I DATI	rev. del 30/03/2011

Sede	Indirizzo
Ufficio del Dirigente Scolastico	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sede	Indirizzo
Ufficio del collaboratore del Dirigente Scolastico e delle funzioni strumentali	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sede	Indirizzo
Ufficio del Direttore dei Servizi Generali ed Amministrativi	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sede	Indirizzo
Ufficio del personale e contabile	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sede	Indirizzo
Ufficio della didattica, protocollo e magazzino	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Sede	Indirizzo
Archivio dati	Via Gandhi 14

Data	Tipo rischio individuato	Danno scarso	Danno medio	Danno alto	Azione correttiva	Firma del R.D.T.

Misure stabilite	Verifica effettuata	Grado di conformità		Rischi evidenziati e Misure correttive	Da completare entro
Censimento dei trattamenti					
Il responsabile del trattamento provvede, ad ogni variazione, a: - redigere ed aggiornare l'elenco dei sistemi di elaborazione connessi in rete e delle tipologie dei trattamenti effettuati - comunicare all'Amministratore di sistema ogni variazione rispetto alla situazione esistente, in particolare ogni modifica del software applicativo (programmi gestionali) o del software di produttività individuale (office, ecc.) e di ogni altro componente presente o di nuova implementazione	E' stata presa visione dell'ultimo censimento dei trattamenti disponibili presso il Responsabile del trattamento e si è verificato che fosse completo	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Il Responsabile del trattamento rende nota o conoscibile ai lavoratori l'identità degli *amministratori di sistema* in relazione ai servizi informatici cui questi sono preposti e con cui vengono effettuati i trattamenti di informazione di carattere personale dei lavoratori stessi, mediante l'intranet di istituto	E' stata presa visione delle comunicazioni effettuate	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Designazione dell'Amministrazione di sistema					
Il documento con cui viene designato l'Amministratore di sistema:	E' stata acquisita copia della nomina				
riporta esperienza, capacità e affidabilità della persona chiamata a ricoprire il ruolo di Amministratore di sistema con riferimento e alle qualità tecniche , professionali e di condotta che costituiscono garanzia del rispetto delle disposizioni		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			

previste dalla normativa in materia di protezione dei dati personali					
reca l'elencazione analitica degli ambiti di operatività consentiti, indicati per settori o per aree applicative, in base al profilo di autorizzazione assegnato		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
indica la descrizione puntuale delle funzioni e dei compiti attribuiti, evitando l'attribuzione di ambiti insufficientemente definiti		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
indica le "verifiche" che il Titolare svolgerà sulle attività svolte dall'Amministratore di sistema e la scadenza delle stesse		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
precisa se la nomina ed il relativo nominativo saranno comunicati al personale in relazione al fatto che i servizi informatici cui questi sono preposti consentono di acquisire informazioni di carattere personale dei lavoratori		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Elenco degli amministratori					
Nel documento programmatico della sicurezza, da mantenere aggiornato e a disposizione del Garante in caso di accertamenti, sono inseriti gli estremi identificativi (nome, cognome, funzione o area organizzativa di appartenenza) degli amministratori di sistema e l'elenco delle funzioni loro attribuite	E' stato acquisito il DPS e l'allegato relativo all'elenco degli amministratori	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Per i servizi di amministrazione di sistema affidati in outsorcing, il Titolare dell'azienda affidataria viene informato dell'obbligo di: - conservare direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema - comunicare all'Istituto l'elenco dei relativi "amministratori di sistema" - aggiornare la lista degli amministratori di	E' stata verificata la presenza delle specifiche clausole a riguardo nei contratti di outsourcing stipulati. E' stata presa visione degli elenchi forniti	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			

sistema ad ogni variazione	dagli outsourcer				
Registrazione degli accessi					
E' adottato il sistema (software) in ambiente Windows: **AdS-LOG, AdS-LOG MANAGER** e n. 2 caselle di posta certificata **PEC**, per la registrazione degli accessi logici (access log) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso)	E' stata presa visione del sistema AdS-LOG; AdS-LOG MANAGER e PEC e del manuale che ne descrive le caratteristiche	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Il sistema AdS-LOG di gestione dei log: - registra in modo completo gli access log, compresi i riferimenti temporali e la descrizione dell'evento che li ha generati da ogni server e pc Il sistema AdS LOG MANAGER di gestione dei log: - mantiene copia inalterabile degli access log, installato su server, intercetta, raggruppa e invia i log Il sistema PEC di gestione dei log: - ammette la possibilità di verificare la loro integrità (account di posta necessari per l'invio con data certa e ricevute di invio, accettazione e inoltro con valore legale "raccomandata AR"	E' stata presa visione del sistema AdS-LOG; AdS-LOG MANAGER e PEC e del manuale che ne descrive le caratteristiche	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Il log degli accessi relativi agli amministratori di sistema è protetto con credenziali specifiche che - sono custodite in cassaforte dal Responsabile del trattamento in busta sigillata, datata e siglata; - - sono conservate per 12 mesi in condizioni di ragionevole sicurezza e con strumenti adatti.	E' stata presa visione delle credenziali riservate custodite dal Responsabile del trattamento	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
I log sono conservati per sei mesi	Sono stati visionati i log	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Operato degli Amministratori di sistema					

L'Amministratore di sistema ha cooperato nella predisposizione ed aggiornamento annuale del documento programmatico sulla sicurezza per la parte concernente il sistema informatico ed il trattamento informatico dei dati e la definizione delle procedure interne inerenti la sicurezza	E' sta fatta l'analisi dei malfunzionamenti segnalati e dei tempi di soluzione registrati.	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'amministratore di sistema ha monitorato il funzionamento della rete e lo stato dei sistemi; con particolare attenzione alla sicurezza informatica, per assicurarne costante efficienza e disponibilità.		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'Amministratore di sistema ha aggiornato con frequenza annuale i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti (firewall, filtri per la posta elettronica, antivirus, ecc.)		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'amministratore di sistema ha provveduto ad effettuare o organizzare le operazioni di backup e recovery dei dati e delle applicazioni.		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'amministratore di sistema ha adottato procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi.		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'amministratore di sistema ha verificato il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore.		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
L'amministratore di sistema ha cooperato nell'impostazione e gestione operativa del sistema di attribuzione dei codici di accesso agli strumenti informatici e di autorizzazione al trattamento di dati personali, la custodia delle credenziali, predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			

archivi elettronici.					
L'Amministratore di sistema ha verificato costantemente che l'Istituto abbia adottato le misure minime di sicurezza per il trattamento dei dati personali provvedendo in collaborazione con il Responsabile del trattamento dei dati personali agli aggiornamenti eventualmente necessari per adeguare il sistema ad eventuali nuove norme in materia di sicurezza.		□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			
Per i servizi di amministrazione di sistema affidati in outsourcing, viene annualmente richiesta al Titolare dell'azienda affidataria attestazione scritta riguardo: - la verifica del rispetto degli obblighi normativi relativi all'Amministratore di sistema; - l'effettuato controllo della rispondenza dell'azione dell'Amministratore di sistema alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.	Sono state visionate le attestazioni rilasciate dagli outsourcer.	□ Conforme □ Non conforme □ Parzialmente conforme □ Non applicabile			

Il presente documento di verifica della conformità dell'attività dell'amministratore di sistema agli obblighi normativi e all'incarico ricevuto viene allegato al Documento Programmatico sulla Sicurezza.

data 30 Marzo 2011 Il Titolare del trattamento …….