Prot. n. 1054/A7
Faenza 26/03/2010

IL PRESIDENTE

Visto il Decreto Legislativo 30 giugno 2003 n.196 recante "Codice in materia di protezione di dati personali" e, in particolare, gli artt. 34 ss.;

Visto l'allegato B del predetto D.Lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l'Istituto Superiore per le Industrie Artistiche di Faenza (di seguito denominato I.S.I.A.), con sede in Corso Mazzini n. 93, a Faenza, in quanto dotato di autonomia statutaria, ai sensi dell'art. 28 del D.Lgs. n. 196 del 30.06.2003, deve ritenersi titolare del trattamento di dati personali;

Atteso che è tenuto a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D.Lgs. n.196 del 2003, adotta il presente

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

L'I.S.I.A., per l'espletamento della funzione didattica e formativa, raccoglie e tratta dati personali dei soggetti coinvolti nella propria attività istituzionale ovvero dei destinatari della stessa, anche con l'ausilio di soggetti esterni, ai sensi del punto 19 dell'Allegato "B", talchè si precisano i seguenti elementi:

1. Elenco dei trattamenti di dati personali;
2. Elenco dei dati personali di natura comune, sensibile o giudiziaria;
3. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
4. Ambito dei trattamenti;
5. Analisi dei rischi incombenti sui dati;
6. Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
7. Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
8. Programma degli interventi formativi degli incaricati del trattamento.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI.

Finalità:

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

1. adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
2. somministrazione dei servizi formativi;
3. gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);
4. adempimenti assicurativi;
5. tenuta della contabilità;
6. gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n. 150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni".

Fonte dei dati:

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'I.S.I.A., in ragione della produzione di:

1. atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente dei servizi formativi;
2. documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;
3. documentazione bancaria, finanziaria e/o assicurativa;
4. documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

2. ELENCO DEI DATI PERSONALI DI NATURA COMUNE, SENSIBILE O GIUDIZIARIA

Sulla scorta delle precisazioni sopra elencate, l'I.S.I.A., sulla base di una prima ricognizione, fatta salva la possibilità di procedere a successive integrazioni e/o correzioni entro il 31 marzo di ogni anno, dichiara, con riferimento ai destinatari o familiari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'Istituzione, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

a) Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D.Lgs. n. 196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva;

b) Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D.Lgs. n. 196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;

c) Dati sensibili, ai sensi dell'art. 4, comma 1, lett. d) del D.Lgs. n. 196 del 2003;

d) Dati giudiziari, ai sensi dell'art. 4, comma 1, lett. e) del D.Lgs. n. 196 del 2003;

e) Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, ammissioni;

f) Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;

g) Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art. 4 comma 1, lett. e) del D.Lgs. n. 196 del 2003;

h) Dati atti a rilevare la presenza presso l'I.S.I.A. dei destinatari dell'offerta formativa ovvero dei familiari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale attività offerta;

i) Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

k) Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;

l) Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;

m) Dati contabili e fiscali;

n) Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni registrati, mobili o immobili;

o) Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

L'Ente titolare del trattamento dei dati ha provveduto ad individuare (come da lettere di incarico allegate al presente Documento) gli incaricati, autorizzandoli al trattamento dei dati in possesso dell'I.S.I.A., esclusivamente con riferimento all'espletamento delle funzioni istituzionali ad essi rispettivamente assegnate.

Tali incaricati, in particolare, sono edotti in merito alla circostanza che:

a) il trattamento e la conservazione dei dati deve avvenire esclusivamente in modo lecito e proporzionato alle funzioni istituzionali, nel rispetto della riservatezza;

b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;

c) integra onere dell'incaricato la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni;

d) integra inosservanza delle istruzioni la comunicazione dei dati in possesso, effettuata in qualsiasi maniera, con eccezione del caso che il destinatario sia l'interessato alle stesse, ovvero altri soggetti legittimati a ricevere dette comunicazioni.

Tutti gli incaricati destinati al trattamento di dati mediante strumento elettronico, sono in possesso di password di accesso alla propria postazione informatica e saranno, successivamente, resi titolari di credenziali di autenticazioni (art. 34, comma 1, lett. b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B. Sarà inoltre designato l'incaricato della custodia delle copie delle credenziali di autenticazione nonché della funzione di verifica del loro aggiornamento periodico ovvero della corretta utilizzazione.

Le suddette credenziali, una volta attivate, saranno disattivate automaticamente periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 mesi.

Al fine di meglio precisare la suddetta ripartizione delle funzioni si rinvia alla tabella seguente

Tabella 1 Strutture preposte ai trattamenti e riparto delle responsabilità

STRUTTURA	INCARICATO	TRATTAMENTI OPERATI DALLA STRUTTURA	COMPITI DELLA STRUTTURA
Direzione	Prof. Germano Zanzani	Trattamenti strumentali allo svolgimento dei compiti istituzionali; Trattamenti strumentali alle attività degli organi collegiali interni ed attività connesse ai rapporti con organi pubblici e privati esterni	Acquisizione e caricamento dei dati; consultazione, stampa, comunicazione a terzi dei dati; richiesta di manutenzione tecnica dei programmi utilizzati nel trattamento dei dati; gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)
Direzione amministrativa	Dott.ssa Antonella Maiorello	Trattamenti strumentali allo svolgimento dei compiti di gestione amministrativa (tenuta dei dati connessi all'espletamento di procedimenti amministrativi; attività contrattuale; procedure di bilancio; gestione del personale ATA). Adempimenti connessi alla L. 241/90. Trattamenti strumentali alle attività degli organi collegiali interni ed attività connesse ai rapporti con organi pubblici e privati esterni (supporto ed assistenza agli organi di gestione dell'ISIA, raccolta delle delibere, raccolta degli atti concertati con altre istituzioni pubbliche; rapporti con altri enti)	Come sopra
Direzione dell'Ufficio di Ragioneria	Dott.ssa Maria Paola Argnani	Trattamenti strumentali allo svolgimento dei compiti di gestione contabile-amministrativa (tenuta dei dati connessi all'espletamento di procedimenti amministrativi, tenuta dei rapporti con i fornitori, gestione minute spese, tenuta dei registri contabili, borse di studio allievi, pagamenti vari); aspetti economici e previdenziali per il pagamento dei professionisti esterni, del personale supplente; rapporti con DPT, INPDAP e INPS; mobilità ERASMUS	Come sopra

Segreteria gestionale	Sig.ra Laura Banzola	Trattamenti strumentali allo svolgimento dei compiti istituzionali (gestione della corrispondenza ricevuta ed inviata; tenuta del protocollo generale con conseguente registrazione della posta, anche elettronica o ricevuta via fax, e delle comunicazioni di ufficio in entrata e in uscita); trattamenti strumentali alla gestione delle attività per la Sicurezza (D.Lgs. 626/94 e ss.); assistenza e supporto ad organi interni; trattamenti per la gestione delle presenze e delle assenze del personale docente e ATA; predisposizione atti per personale docente e ATA; gestione documenti giustificativi delle assenze, anche sanitari;trattamenti connessi alla gestione del c/c postale; gestione informatica dell'ufficio	Come sopra
Segreteria finanziaria	Dott.ssa Rossella Gondoni	Trattamenti strumentali allo svolgimento dei compiti istituzionali relativi all'espletamento delle procedure di spesa per acquisti; tenuta dei rapporti con i fornitori; gestione inventario; gestione facile consumo; gestione informatica dell'ufficio	Come sopra
Segreteria didattica	Dott.ssa Laura Merella	Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione, ammissione ed esami; documentazione concernente opzioni per insegnamenti facoltativi; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa; registri relativi alle presenze presso l'istituzione scolastica; tenuta dei fascicoli personali degli allievi); compilazione diplomi, certificati e attestazioni; gestione documenti giustificativi delle assenze, anche sanitari; gestione informatica della segreteria; eventuali dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'attività didattica (per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare).	Come sopra

4. AMBITO DEI TRATTAMENTI.

Atteso che gli uffici di segreteria sono ubicati unicamente nella sede dell'I.S.I.A. in Corso Mazzini n. 93, si precisano le modalità del trattamento dei dati nei vari uffici, mediante strumenti elettronici, secondo le modalità precisate nella tabella sottostante.

Tabella 2 Elenco dei trattamenti: informazioni di base

Struttura deputata al trattamento	Natura dei dati trattati	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Direttore	Dati personali Dati identificativi Dati Sensibili Dati Giudiziari	Stesso ufficio	Ditta esterna, individuata previo espletamento di apposita procedura, limitatamente alle esigenze di manutenzione ordinaria e straordinaria, e/o riparazione del server e dei P.C. interni.	PC interni
Direzione amministrativa	Come sopra	Come sopra	Come sopra	Come sopra
Direzione Ufficio di Ragioneria	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria gestionale	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria didattica	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria finanziaria	Come sopra	Segreteria	Come sopra	Come sopra

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici interni (P.C.) collegati in rete fra loro, e/o mediante collegamenti alla rete internet. Con riferimento alla gestione dei dati per via informatica e telematica mediante rete ministeriale e di altri Enti pubblici (CINECA; S.P.T.-Service Personale Tesoro; S.A.RE.- Semplificazione Amministrativa in Rete; INAIL, INPS ecc.), l'I.S.I.A. declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni trasmesse ed ivi contenute e gestite.

Con riferimento all'ubicazione fisica dei supporti di memorizzazione delle copie di sicurezza si precisa che sono attivi presso l'I.S.I.A. un SERVER configurato con sistema RAID 5 più DISCO SPIRE ed un secondo SERVER di back up. Sono effettuate copie di sicurezza giornaliere su nastro LTO2 che si conservano in armadio blindato. Inoltre, annualmente si effettua una copia dei dati affidata ad un dipendente e conservata all'esterno.

La tabella seguente riassume il quadro dei trattamenti secondo modalità e tipologia, precisando l'ubicazione dei supporti di memorizzazione.

Tabella 3 Elenco dei trattamenti: descrizione degli strumenti utilizzati

IDENTIFICATIVO DEL TRATTAMENTO	EVENTUALE BANCHE DATI DI SUPPORTO	UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E DELLE COPIE DI SICUREZZA	TIPOLOGIA DI DISPOSITIVI DI ACCESSO	TIPOLOGIA DI INTERCONNESSIONE
Direzione	Archivi ISIA	SERVER configurato con sistema RAID 5 più DISCO SPIRE ubicato in apposito locale ed un secondo SERVER di back up ubicato presso l'ufficio della Direzione. Sono effettuate copie di sicurezza giornaliere su nastro LTO2 che si conservano in armadio blindato presso l'ufficio della segreteria finanziaria. Inoltre, annualmente si effettua una copia dei dati affidata ad un dipendente e conservata all'esterno.	PC	- Hardware e software - Rete locale e internet

Direzione a.mm.va	Archivi ISIA	Come sopra	Come sopra	Come sopra
Direzione Ufficio di Ragioneria	Archivi ISIA	Come sopra	Come sopra	Come sopra
Segreteria Didattica	Archivio degli studenti Archivi ISIA per quanto necessario	Come sopra	Come sopra	Come sopra
Segreteria finanziaria	Archivio delle imprese fornitrici di servizi e/o prestazioni. Archivi ISIA per quanto necessario	Come sopra	Come sopra	Come sopra
Segreteria gestionale	Archivio generale di entrata e uscita Archivio dei dipendenti. Archivi ISIA per quanto necessario	Come sopra	Come sopra	Come sopra
Tutti gli archivi sono contenuti negli elaboratori, sottoposti, sistematicamente, a revisione o manutenzione da parte di ditta esterna, incaricata dell'assistenza periodica e sistematica per interventi sia in caso di trasporto dell'elaboratore all'esterno dell'ente, presso i locali della ditta, sia in caso di intervento sul posto, presso la sede dell'Istituto.				

5. ANALISI DEI RISCHI INCOMBENTI SUI DATI

L'I.S.I.A. ha proceduto ad una ricognizione dei rischi che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuiti, in grado di recare pregiudizio ai dati personali trattati.

Le fonti di rischio sono state accorpate in:

1) Comportamenti degli operatori.

Sottrazione di credenziali di autenticazione, quando attivate; comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati; comportamenti dolosi dei soggetti legittimati; errori materiali.

2) Eventi relativi agli strumenti.

Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software), spamming o tecniche di sabotaggio. Malfunzionamento, indisponibilità o usura fisica degli strumenti. Accessi abusivi negli strumenti elettronici. Intercettazione dei dati in occasione di trasmissione in rete.

3) Eventi relativi al contesto fisico-ambientale.

Distruzione o perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, seppur astrattamente preventivabili (incendi o allagamenti), di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele. Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica per lunghi periodi di tempo, in grado di pregiudicare la climatizzazione dei locali. Furto o danneggiamento degli strumenti elettronici di trattamento dei dati, in orario diverso da quello di lavoro. Accesso non autorizzato da parte di terzi – interni o esterni all'Istituzione – mediante uso abusivo di credenziali di autenticazione, in funzione di danneggiamento o sottrazione dei dati. Errori umani nell'attivazione degli strumenti di protezione.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione presso l'Istituzione, adottando la seguente scansione:

A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Tabella 4 Analisi dei rischi

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE ADOTTATE O DA ADOTTARE
		DESCRIZIONE	GRAVITÀ STIMATA	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione, quando attivate	Accesso altrui non autorizzato	M	Misura da adottare quando saranno attivate le credenziali di autenticazione: vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Misura adottata: adeguate formazione e informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	M	Misura adottata: vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	M	Misura adottata: vigilanza sul rispetto delle istruzioni impartite, formazione e informazione adeguate
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori	MA	Misure di sicurezza adottate: - antivirus - accesso autorizzato ad utenti esterni per l'installazione di nuovi software - firewall fisico
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Adozione di idonei dispositivi di protezione
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Misura adottata: assistenza e manutenzione continua e sistematica degli elaboratori e dei programmi; ricambio periodico

	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**MA**	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	**MA**	Adozione di idonei dispositivi di protezione
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Misura adottata: protezione dell'edificio con attività di vigilanza del personale addetto. Protezione dei singoli locali mediante chiusura degli stessi con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	**MB**	Protezione dell'edificio con attività di vigilanza del personale addetto. Protezione dei singoli locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante chiusura degli stessi con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	**M**	Attività di prevenzione, controllo, assistenza e manutenzione periodica,vigilanza sul rispetto delle istruzioni impartite, formazione informazione adeguate

	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**A**	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e informazione adeguate

6. MISURE ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI, NONCHÈ LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ.

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

Tabella 5 Le misure di sicurezza adottate o da adottare

MISURA	RISCHIO CONTRASTATO	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIÀ IN ESSERE	PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Direzione	Archivi	1)SERVER configurato con sistema RAID 5 più DISCO SPIRE ubicato in apposito locale ed un secondo SERVER di back up ubicato presso l'ufficio della Direzione. Sono effettuate copie di sicurezza giornaliere su nastro LTO2 che si conservano in armadio blindato presso l'ufficio della segreteria finanziaria.	1) settimanale 2) settimanale 3) semestrale 4) semestrale 5) gestito da RUBA Responsabile pro tempore del servizio – ditta esterna DECA SYSTEM. Si prevede di adottare la misura di copia dei dati da conservare all'esterno con periodicità semestrale.

				Inoltre, annualmente si effettua una copia dei dati affidata ad un dipendente e conservata all'esterno. 2) Antivirus 3) Firewall 4) Firewall di back up 5) Antispam	2) settimanale 3) semestrale 4) semestrale 5) gestito da RUBA Responsabile pro tempore del servizio – ditta esterna DECA SYSTEM. Si prevede di adottare la misura di copia dei dati da conservare all'esterno con periodicità semestrale anziché annuale
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Direzione Amm.va	Come sopra	Come sopra	Come sopra
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Direzione Ufficio di Ragioneria	Come sopra	Come sopra	Come sopra

Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria didattica	Come sopra	Come sopra	Come sopra
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria gestionale	Come sopra	Come sopra	Come sopra
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria finanziaria	Come sopra	Come sopra	Come sopra

7. CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI A SEGUITO DI DISTRUZIONE O DANNEGGIAMENTO

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita si è proceduto a definire una procedura di quotidiana esecuzione di copie di sicurezza, acquisizione delle licenze d'uso per software antivirus, nonché sistemi di firewall e antispam con verifica di idoneità e costante aggiornamento degli stessi. In particolare l'aggiornamento relativo all'antivirus viene effettuato quotidianamente tramite controllo centralizzato. In ogni caso, si osserva che l'Istituto durante l'orario di apertura giornaliero controlla gli accessi ai locali mediante personale interno (coadiutori). I documenti sono anche conservati in copia cartacea presso gli stessi locali dell'I.S.I.A. non accessibili ai terzi e dotati di strumenti di protezione (stanze chiuse a chiave, armadi con serrature).

Semestralmente ciascuna postazione informatica è sottoposta ad IMMAGINE DEL DISCO.

Sinteticamente è possibile rappresentare la seguente procedura di copia, verifica e ripristino dei dati per ogni P.C.

Tabella 6 Procedure di copia, verifica e ripristino adottati per ogni singola unità contenente dati

Struttura in possesso di P.C.	Applicativo	Sistema operativo	Procedura di copia	Procedura di verifica	Ripristino
Direzione	Office	Windows XP Professional	Tramite SERVER	Tramite SERVER	Tramite doppio SERVER; nastro LTO2; immagine del disco semestrale
Direzione amm.va	Come sopra	Come sopra	Come sopra	Come sopra	Come sopra
Direzione Ufficio Ragioneria	Come sopra	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria gestionale	Come sopra	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria didattica	Come sopra	Come sopra	Come sopra	Come sopra	Come sopra
Segreteria finanziaria	Come sopra	Come sopra	Come sopra	Come sopra	Come sopra

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

Tabella 7 Salvataggio dei dati

SALVATAGGIO		CRITERI INDIVIDUATI PER IL SALVATAGGIO	UBICAZIONE DI CONSERVAZIONE DELLE COPIE	MODALITA' DEL SALVATAGGIO
STRUTTURA	DATI IDENTIFICATIVI, SENSIBILI O GIUDIZIARI			
Direzione	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Salvataggio dati giornaliero	Server posto in locale apposito con serratura e chiavi distribuite ai soli autorizzati; 2° server di back up presso ufficio di Direzione; copie di sicurezza giornaliere su nastro LTO2 conservato in armadio blindato presso l'ufficio della segreteria finanziaria. Annualmente si effettua una copia dei dati affidata ad un dipendente e conservata all'esterno.	Programmazione di salvataggio dati automatico quotidiano sul 1° server; salvataggio dati automatico ogni 15 gg. sul 2° server; nastro LTO2 quotidiano; copia all'esterno annuale.
Direzione amm.va	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Come sopra	Come sopra	Come sopra

Direzione Ufficio di Ragioneria	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Come sopra	Come sopra	Come sopra
Segreteria gestionale	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Come sopra	Come sopra	Come sopra
Segreteria didattica	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Come sopra	Come sopra	Come sopra
Segreteria finanziaria	Dati identificativi in generale Stato di salute Adesione a sindacati Origine razziale o etnica Confessione religiosa Dati giudiziari	Come sopra	Come sopra	Come sopra

Con riferimento alle procedure di ripristino, nell'ipotesi di distruzione o danneggiamento, l'Istituzione ha già adottato o adotterà le seguenti modalità:

TABELLA 8 RIPRISTINO DEI DATI

RIPRISTINO (in seguito a distruzione o danneggiamento)		
DATA BASE/ARCHIVIO	**SCHEDA OPERATIVA**	**PIANIFICAZIONE DELLE PROVE DI RIPRISTINO**
Direzione	Sono 3 i livelli di operazioni previsti per il ripristino: 1) recupero dati dal 1° Server; 2) se la 1^ operazione non è possibile, recupero dati dal 2° server; 3) se neanche la 2^ operazione è possibile, recupero dati dal nastro LTO2.	Annuale
Direzione amministrativa	Come sopra	Come sopra
Direzione Ufficio Ragioneria	Come sopra	Come sopra
Segreteria didattica	Come sopra	Come sopra
Segreteria gestionale	Come sopra	Come sopra
Segreteria finanziaria	Come sopra	Come sopra

8. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO.

L'I.S.I.A. intende aderire alle iniziative formative eventualmente organizzate dalla direzione regionale del Ministero dell'Istruzione dell'Università e della Ricerca Scientifica, tenendo anche conto dell'economicità di un'azione organizzata su base regionale, rispetto ad una gestione in proprio delle attività formative. L'Istituzione opera integrale rinvio alla programmazione della Direzione regionale, riservandosi comunque di agire in via suppletiva, qualora, per ragioni organizzative od economiche, non sia possibile far partecipare il proprio personale alle attività di formazione necessarie per adempiere alle prescrizioni ordinamentali.

Tabella 9 Pianificazione degli interventi formativi

CORSO DI FORMAZIONE (OGGETTO)	DESCRIZIONE SINTETICA DELL'OBIETTIVO FORMATIVO	CLASSI DI INCARICO INTERESSATE	INCARICATI INTERESSATI	INCARICATI GIÀ FORMATI/DA FORMARE NEL CORSO DELL'ANNO	CALENDARIO
L'adempimento dell'obbligo di aggiornamento del DPS	Porre in condizione il personale competente di adempiere entro il 31 marzo di ogni anno all'obbligo di aggiornamento del DPS	Tutti gli incaricati del trattamento	Personale amministrativo	Personale amministrativo	Da concordare con la direzione regionale. In mancanza, azione suppletiva dell'Istituto
Quadro riepilogativo degli adempimenti e degli obblighi in materia di privacy (ivi incluse le misure di sicurezza per gli archivi cartacei)	Mantenimento del richiesto grado di conoscenza dell'intero impianto della normativa in materia di privacy, anche ai fini delle misure di sicurezza da adottare per gli archivi cartacei.	Tutto il personale amministrativo.	Come sopra	Come sopra	Come sopra
Privacy e diritto di accesso nelle istituzioni scolastiche	Fornire un quadro coordinato dei diritti (di accesso e alla riservatezza) riconosciuti all'utenza dalla vigente legislazione, in rapporto ai doveri gravanti sulle strutture scolastiche	Responsabili dei servizi e personale a diretto contatto con l'utenza	Come sopra	Come sopra	Come sopra
Esame della casistica ricorrente nell'attività di ufficio, alla luce delle sentenze del giudice amministrativo e dei pronunciamenti del Garante	Aggiornare il personale sull'eventuale sopravvenuta evoluzione dell'interpretazione della normativa	Responsabili dei servizi e personale a diretto contatto con l'utenza	Come sopra	Come sopra	Come sopra

9. ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI

I trattamenti di dati personali con strumenti diversi da quelli elettronici sono effettuati dagli incaricati seguendo le istruzioni ad essi impartite con le lettere di incarico, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ha carattere annuale. Gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
L'I.S.I.A. si riserva di valutare l'opportunità e la convenienza di procedere alla esternalizzazione di taluni trattamenti, secondo le modalità conformi a quanto previsto dal D.Lgs. n. 196 del 2003, procedendo alla eventuale nomina di un soggetto esterno quale responsabile del trattamento, limitatamente ai dati e alle operazioni necessari per lo svolgimento delle eventuali attività che si riterrà di conferire. In tale ipotesi l'I.S.I.A. provvederebbe ad imporre le adeguate cautele affinché il soggetto destinatario adotti le misure di sicurezza richieste dal Codice, ivi incluso il relativo all. B.

10. SISTEMA DI AUTORIZZAZIONE.

Al momento, considerata la forte carenza di personale e le esigenze organizzative dell'ente, per il cui ordinario funzionamento è indispensabile assicurare una certa interscambiabilità funzionale degli incaricati, non è stato adottato un sistema di autorizzazione.

11. OBBLIGO DI AGGIORNAMENTO PERIODICO DEL DPS

Il presente documento programmatico sulla sicurezza è sottoposto a revisione annuale nella sua interezza, entro la scadenza del 31 marzo di ciascun anno, come previsto dalla regola 19 del Disciplinare tecnico di cui all'allegato B) al D.Lgs. 196/03, in relazione al disposto dell'art. 34, lettera g) del decreto stesso.

Gli allegati al presente documento ne formano parte integrante.

IL PRESIDENTE
TITOLARE DEL TRATTAMENTO
Prof.ssa Anty Pansera

ESTRATTO VERBALE DI DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE
DELIBERA N. 8
(dal Verbale n. 3 del 07/04/2010)

1. **OGGETTO:Approvazione Documento Programmatico sulla Sicurezza: Privacy – D.Lgs. 30/06/2003 n. 196 e s.m. e/o i.**

Addì 07/04/2010, alle ore 14.30, presso i locali dell'Istituto, si è riunito il Consiglio di Amministrazione dell'I.S.I.A. di Faenza, in seguito alla convocazione di cui alla nota prot. n. 1045/A19a del 26/03/2010, per discutere i sotto elencati punti iscritti all'ordine del giorno della seduta:

Comunicazioni del Presidente.
Comunicazioni del Direttore

2. Celebrazione trentennale ISIA: sviluppi programma ed organizzazione
3. Approvazione verbale seduta precedente del 25/02/2010
4. Approvazione Regolamento utilizzo carte di credito e prepagate.
5. Approvazione Documento Programmatico sulla Sicurezza: Privacy – D.Lgs. 30/06/2003 n. 196 e s.m. e/o i.
6. Varie ed eventuali.

All'appello dei componenti risulta quanto segue:

N°	*Nominativi*	COMPONENTE CDA	PRESENTI
1	Prof.ssa Anty Pansera	PRESIDENTE	SI
2	Prof. Germano Zanzani	DIRETTORE	SI
3	Prof.ssa Daniela Lotta	DOCENTE	SI
4	Sig. Robert Corbari	STUDENTE	SI
5	Assessore Germano Savorani	RAPPR. PROVINCIA RA.	NO
6	Dott.ssa Francesca Foschi	ESPERTO ESTERNO	SI
Totale dei presenti			**5**

Il dott. Germano Savorani è assente giustificato per improrogabili impegni di lavoro.

E' presente, inoltre, il Direttore amministrativo dott.ssa Antonella Maiorello con funzioni di Segretario e voto consultivo, ai sensi dell'art 7, comma 5 dello Statuto.

Il Consiglio di Amministrazione,
Preso Atto della propria composizione come di seguito elencata:
- Presidente: Anty Pansera – decreto MIUR 17/02/2010
- Direttore: Germano Zanzani – decreto MIUR del 12/07/2007
- Componente docenti: Daniela Lotta – decreto MIUR del 29/07/2008
- Componente studenti: Roberto Corbari – decreto MIUR n. 15 del 27/01/2009
- Componente esterno, rappresentante Ente Locale Provincia di Ravenna dott. Germano Savorani – decreto MIUR del 22/09/2008
- Componente esperto esterno: Francesca Foschi – decreto n. 161 del 23/11/2009.

Preso Atto dell'art. 7, commi 1-8, dello Statuto relativamente alla composizione e alle competenze del Consiglio di Amministrazione;
Preso Atto del Regolamento sul funzionamento del Consiglio di Amministrazione dell'ISIA di Faenza approvato con delibera CDA-2009 n. 13 del 06/05/2009 ed emanato con decreto presidenziale n. 61 (prot. n. 1528/A19 del 07/05/2009);

Ministero Università e Ricerca - MUR
Alta Formazione Artistica Musicale
48018 Faenza RA
Corso Mazzini, 93
tel. +39 0546 22293
+39 0546 686490
fax +39 0546 665136
C.f. 90000140393
www.isiafaenza.it
info@isiafaenza.it

Preso Atto che le funzioni di Segretario sono affidate alla dott.ssa Antonella Maiorello, nella sua qualità di Direttore amministrativo, ai sensi dell'art. 7, comma 5, dello Statuto;

SI RIUNISCE UFFICIALMENTE

e il Presidente, Prof.ssa Anty Pansera, riconosciuta la validità della riunione, data l'esistenza del numero legale, in considerazione della totalità delle presenze dei componenti il Consiglio di Amministrazione, dichiara aperta la seduta per la trattazione degli argomenti oggetto della convocazione.

.....OMISSIS.....

8. <u>Approvazione Documento Programmatico sulla Sicurezza: Privacy – D.Lgs. 30/06/03 n. 196 e s.m. e/o i.</u>

Il Consiglio di Amministrazione,
- visto il D.Lgs. 196/03 (cd. Codice in materia di protezione dei dati personali) ed il relativo allegato tecnico (allegato B) in materia di misure minime di sicurezza;
- visto, in particolare, l'art. 19 del predetto allegato B che fissa al 31 marzo di ogni anno la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza;
- visto il Documento Programmatico sulla Sicurezza approvato in prima stesura con delibera n. 11 - CdA del 30/03/2009;
- considerato l'obbligo per l'ISIA di porre in essere gli atti dovuti in osservanza della normativa vigente in materia di Privacy,

all'unanimità,

Delibera n. 8 – 2010 CdA

di approvare l'aggiornamento del Documento Programmatico per la Sicurezza in materia di Privacy, con il testo esaminato nella presente seduta, demandando al Presidente, nella sua qualità di Titolare del trattamento dei dati personali gestiti da questo ISIA, di provvedere all'emanazione dello stesso ed al conferimento degli incarichi per il trattamento dei dati al personale interessato.

DELIBERA SEDUTA STANTE

.....OMISSIS.....

Alle ore 16.20 del giorno 07/04/2010, conclusa la trattazione degli argomenti iscritti all'ordine del giorno di cui alla nota 1045/A19A del 26/03/2010, la Prof.ssa Anty Pansera, che ha presieduto la seduta, dichiara conclusi i lavori.
Di quanto sopra si è redatto il presente verbale che, previa lettura e conferma, viene sottoscritto come appresso.

F.to Il Direttore amministrativo
dott.ssa Antonella Maiorello

F.to IL PRESIDENTE
Prof.ssa Anty Pansera

Ministero Università e Ricerca - MUR
Alta Formazione Artistica Musicale
48018 Faenza RA
Corso Mazzini, 93
tel. +39 0546 22293
+39 0546 686490
fax +39 0546 665136
C.f. 90000140393
www.isiafaenza.it
info@isiafaenza.it