POLICY INTERNA DI
SMALTIMENTO RIFIUTI RAEE

INFORMAZIONI SUL DOCUMENTO		
Data:	01/10/2018	
Azienda:	**Istituto Comprensivo Della Val Nure** Via Francesco Acerbi n. 61 29028 Ponte dell'Olio (PC) C.F. 80010070334	
Rif. Doc.:	Procedura di gestione delle misure minime di sicurezza (misure_sicrezza.pdf)	
Versione:	01.01	
Redatto da:	GALLI DATA SERVICE di Gregorio Galli (DPO)	
Revisionato da:		
Approvato da:	**Istituto Comprensivo Della Val Nure** (Titolare del trattamento) In persona di: **Teresa Andena** (Dirigente Scolastica Reggente)	…….. (TIMBRO E FIRMA)

INDICE

1. AMBITO NORMATIVO DI RIFERIMENTO

- D.LGS. 03/04/2006 N°152 ("Codice ambientale")
- D.LGS. 14/03/2014 N° 49
- D. LGS. 20/11/2008 N° 188
- D.LGS. 196/2003 T.U. Privacy, come novellato dal D. Lgs. 101/2018
- PROVVEDIMENTO 13/10/2008 pubblicato in G.U. N°287 del 09/12/2008
- SCHEDA INFORMATIVA DEL 12/12/2008

Il D.Lgs. 03/04/2006 ed i citati D.M. mirano tra l'altro a promuovere il reimpiego, il riciclaggio ed altre forme di recupero, così da **ridurre al minimo** le apparecchiature elettriche ed elettroniche da inviare allo smaltimento.

Tuttavia nessuna di tali norme esime il Titolare del trattamento dagli obblighi e dalle responsabilità della sicurezza dei dati contro **accessi non autorizzati**. Una responsabilità che può essere sia **penale** (Art.169 del T.U. Privacy) che **civile** in caso di danni a terzi (Art. 15 T.U. Privacy e Codice Civile).

Gli elaboratori elettronici (computer, server, ecc.), ma anche supporti rimovibili (CD-Rom, DVD, Chiavette, HD, ecc.) reimpiegati, riciclati o dismessi possono contenere nomi, indirizzi, mail, documenti ed in generale dati personali che espongono al **rischio di manipolazione di dati e furto di identità**.

Il Garante Privacy ha perciò adottato il Provvedimento del 13/10/2008 "Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali", teso a facilitare una **effettiva cancellazione** dei dati dalle apparecchiature.

Vengono inoltre elencate tramite scheda informativa (Doc.Web:1574080 del 12/12/2008) **istruzioni pratiche** per una cancellazione sicura dei dati.

2. MODALITA' DI PROTEZIONE DEI DATI IN CASO DI REIMPIEGO, RICICLO O SMALTIMENTO DI APPARECCHIATURE O SUPPORTI

Il problema dell'**e-waste** riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a sé o a terzi: è infatti compito del loro possessore assicurare che questi dati non possano andare dispersi e acquisiti, anche in modo incontrollato, da estranei.

Per prevenire l'acquisizione indebita dei dati occorre operare in diversi modi/tempi secondo le circostanze:

- **preventivamente**, con tecniche di memorizzazione sicura;
- **immediatamente prima della cessione o dismissione**, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- **al momento della cessione o dismissione**, con la demagnetizzazione (degaussing) che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

REIMPIEGO	RICICLAGGIO	SMALTIMENTO
Memorizzazione sicura	Memorizzazione sicura	Memorizzazione sicura
Cancellazione sicura	Cancellazione sicura	Cancellazione sicura
		Distruzione

3. MEMORIZZAZIONE SICURA

La memorizzazione sicura dei file si può realizzare sui più diffusi sistemi operativi con l'attivazione di **funzionalità crittografiche** proprie del sistema, se disponibili, o con l'installazione di prodotti software aggiuntivi. Le concrete modalità dipendono fortemente dallo specifico **sistema operativo** utilizzato e talvolta anche dalla sua versione o dall'applicazione di patch e aggiornamenti.

MISURE TECNICHE PREVENTIVE:

- Cifratura di file o gruppi di file con parole chiave riservate
- Cifratura automatica al momento della scrittura, con parola chiave riservata al solo utente

AMBIENTE MICROSOFT	AMBIENTE APPLE	ALTRE PIATTAFORME
Procedure descritte nelle pagine informative predisposte http://www.microsoft.com/italy/pmi/sicurezza/privacy	Funzionalità **FileVault** disponibili nel sistema operativo Mac OS X http://www.apple..com/support/?path=Mac/10.4/it/mh1877.html	**Sw TrueCrypt**, che offre funzioni di cifratura con strong encryption di partizioni o interi dischi http://www.truecrypt.org

4. CANCELLAZIONE SICURA

La **semplice cancellazione** dei file o la **formattazione** dell'Hard-Disk non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili. Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze.

MISURE TECNICHE DI CANCELLAZIONE SICURA:

- Programmi informatici (wiping program, file shredder) che, una volta cancellati i dati con normale procedura, sugli spazi resi vuoti scrivono ripetutamente sequenze casuali di cifre binarie, riducendo al minimo la possibilità di recupero delle informazioni;
- Formattazione a basso livello, tenendo conto delle istruzioni del produttore dei dispositivo e delle possibili conseguenze (es. inutilizzabilità).

AMBIENTE MICROSOFT	AMBIENTE APPLE	ALTRE PIATTAFORME
Procedure descritte nelle pagine informative predisposte http://www.microsoft.com/italy/pmi/sicurezza/privacy	Il sistema operativo Mac OS X incorpora una funzione di "svuotamento del cestino in modalità sicura" oppure ricorrere ad utility di tipo "open source" come **Permanent Eraser**, che consente di effettuare cancellazioni sicure con algoritmo avanzato	Per i sistemi Unix e Linux un software tra i più noti ed efficaci è DBAN (**Dark's Boot and Nuke**), che consente di cancellare un hard-disk funzionante su un personal computer dotato di lettore CDRom o di DVD. (www.dban.org/download)

5. DISTRUZIONE SICURA

MISURE TECNICHE DI DISTRUZIONE SICURA:

PUNZONATURA O DEFORMAZIONE	DISTRUZIONE O DISINTEGRAZIONE	DEMAGNETIZZAZIONE AD ALTA INTENSITA'
Gli hard-disk possono essere **resi inutilizzabili** aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento	I supporti ottici a sola lettura (CDRom, DVD) possono essere distrutti o polverizzati con apposite macchine, analoghe ai trita carta in uso negli uffici.	Tramite utilizzo di degausser che permettono l'azzeramento della aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici

6. MODALITA' OPERATIVE

Gli accorgimenti dettati dal Garante possono essere attuati da risorse interne qualificate o con l'incarico di soggetti terzi, tecnicamente competenti (es. centri di assistenza, produttori/distributori, ecc.) che si impegnino ad effettuarli o che attestino di averli effettuati.

FINALITA'	MODALITA'	A CURA DI
Reimpiego o riciclo apparecchiature	( ) Cifratura file ( ) Cifratura scrittura (X) Cancellazione sicura (X) Formattazione	Titolare. Specifici incaricati.
Smaltimento apparecchiature	( ) Cifratura file ( ) Cifratura scrittura (X) Cancellazione sicura (X) Formattazione (X) Punzonatura / deformazione (X) Distruzione / Disintegrazione ( ) Demagnetizzazione alta intensità (X) Rimozione del supporto di memoria	Titolare. Specifici incaricati.

La tabella riporta le modalità operative che l'organizzazione può adottare al fine di garantire un corretto smaltimento o riutilizzo degli strumenti contenenti dati.

Gli interventi indicati nella colonna "MODALITÀ"si riferiscono alle indicazioni dettagliate nelle precedenti tabelle, a seconda delle peculiarità delle apparecchiature da smaltire.

Il Titolare dei trattamenti potrà a sua discrezione tenere un "registro RAEE" in cui catalogare cronologicamente le apparecchiature reimpiegate/smaltite e le modalità adottate.

In caso di affidamento di RAEE a soggetti terzi sarà cura del Titolare richiedere l'adozione delle misure indicate nella presente policy.

6. REVISIONE DELLA POLICY

Il presente documento è oggetto di revisione periodica, in relazione ad eventuali:

- modifiche delle modalità organizzative interne;
- variazioni della normativa di riferimento.