Allegato alla Delibera del Consiglio di Istituto nr.05 del …….

MANUALE DI GESTIONE DOCUMENTALE
ISTITUTO COMPRENSIVO BASSA ATESINA

FEBBRAIO 2017

INDICE

1. Principi generali e organizzativi

1.1 Ambito di applicazione e normativa di riferimento

Il presente *Manuale di gestione documentale* è adottato dall' Istituto Comprensivo Bassa Atesina (di seguito denominato "scuola") ai sensi dell'articolo 5 del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione digitale di cui al decreto legislativo n. 82 del 2005".
Il Manuale descrive il sistema di gestione dei documenti informatici, anche ai fini della conservazione, e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Il Manuale è da intendersi quale strumento di lavoro e di riferimento per gli utenti del protocollo informatico della scuola per la corretta gestione dei documenti in tutto il loro ciclo di vita.
Si precisa che, ai fini della redazione del presente Manuale, la scuola si attiene alla normativa vigente in materia riportata nell'allegato n. 1.

1.2 Area organizzativa omogenea (AOO) e registro unico di protocollo

La scuola ha individuato al suo interno un'unica area organizzativa omogenea (AOO), alla quale corrisponde un registro unico di protocollo, denominato "Registro 25900 IC Bassa Atesina"
Il registro di protocollo della scuola presenta le caratteristiche del protocollo informatico ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modifiche, e del suindicato decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013.

1.3 Organizzazione del protocollo

La protocollazione avviene presso la Segreteria dell'Istituto. Le abilitazioni alla protocollazione sono assegnate dal/la Dirigente Scolastico/a.

1.4 Casella di posta elettronica certificata della scuola (PEC)

La casella di posta elettronica certificata (PEC) della scuola è: IC.BassaAtesina@pec.prov.bz.it.
L'indirizzo della casella di posta elettronica certificata della scuola è pubblicato nell'Indice delle Pubbliche Amministrazioni, di seguito Indice PA (http://www.indicepa.gov.it), e sul sito web della scuola www.ic-bassa-atesina.it.

1.5 Caselle di posta elettronica ordinaria

L'indirizzo istituzionale della casella di posta elettronica ordinaria della scuola è ic.bassaatesina@scuola.alto-adige.it. L'indirizzo della casella di posta elettronica ordinaria è pubblicato sul sito web della scuola www.ic-bassa-atesina.it.

2. Documento informatico

2.1 Formazione dei documenti informatici

La scuola forma gli originali dei propri documenti come documenti informatici, nel rispetto delle disposizioni del Codice dell'Amministrazione Digitale (decreto legislativo 7 marzo 2005, n. 82, e successive modifiche) e delle relative regole tecniche.

I documenti informatici possono essere formati:

- mediante strumenti informatici di elaborazione testi (per es. Microsoft Word, LibreOffice, ecc.);
- mediante applicazioni informatiche che gestiscono procedimenti amministrativi e producono automaticamente i documenti.

Il documento deve riportare sempre una data, che deve coincidere con la data della sottoscrizione con firma digitale. Nel documento deve essere indicato anche il luogo della firma, che deve corrispondere al luogo in cui il documento viene effettivamente firmato.

Si precisa che all'interno del documento informatico non è riportata la segnatura di protocollo, in quanto la protocollazione deve avvenire per legge in un momento successivo alla sottoscrizione del documento.

Prima della loro sottoscrizione con firma digitale, i documenti informatici sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione, nonché l'immutabilità nel tempo del contenuto e la loro leggibilità.

I formati di file adottati dalla scuola per la formazione dei propri documenti sono elencati nell'allegato n. 2.

All'atto della protocollazione, al documento informatico sono associati i metadati indicati nell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modifiche, e quelli previsti dall'articolo 9 del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 in materia di protocollo informatico.

2.2 Sottoscrizione dei documenti informatici

Completata la fase di redazione del documento, questo deve essere sottoscritto. La sottoscrizione dei documenti informatici della scuola avviene con firma digitale.
La sottoscrizione determina l'assunzione della paternità del contenuto del documento.

Sono attualmente previste tre modalità differenti di sottoscrizione con firma digitale:

- la sottoscrizione del documento attraverso un'applicazione per la firma digitale (per es. Dike);
- la sottoscrizione del documento all'interno di un'applicazione (per es. eLIQ);
- la sottoscrizione del documento con firma automatica massiva remota tramite dispositivo HSM.

Ove risulti necessaria un'altra o più firme, anche queste devono essere apposte con firma digitale.
Nel caso di sigle e visti, questi sono apposti sui documenti mediante firma elettronica semplice (per es. credenziali di identificazione personale).

Qualsiasi dispositivo per la firma digitale (per es. smart card, token USB, OTP-One Time Password, ecc.), così come il codice di accesso al certificato di firma, sono strettamente personali. L'utilizzo del dispositivo e il codice di accesso si presumono riconducibili al/alla titolare e un utilizzo degli stessi da parte di persona diversa costituisce un illecito.
Le credenziali di identificazione personale (username e password) sono anch'esse strettamente personali; l'utilizzo della stesse da parte di persona diversa dal/dalla titolare costituisce un illecito.

I documenti sottoscritti con firma digitale non devono contenere macroistruzioni o codici eseguibili, pena la loro nullità.

3. Registrazione di protocollo

3.1 Registrazione di protocollo

Sono soggetti a registrazione di protocollo tutti i documenti cartacei e informatici aventi rilevanza giuridico-probatoria o amministrativa. Rientrano tra i documenti informatici anche i messaggi di posta elettronica ordinaria e certificata (PEC).

Sono esclusi dalla registrazione di protocollo:

- i bollettini ufficiali e i notiziari della pubblica amministrazione,
- i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni,
- i documenti in elaborazione (bozze),
- la corrispondenza riservata,
- i documenti soggetti a registrazione particolare (per es. decreti del/la Dirigente scolastica, delibere del Consiglio di Istituto, delibere del Collegio dei docenti).

La registrazione di protocollo è consentita solo se è presente il documento in originale e, per quanto concerne i documenti in uscita e interni, se i documenti sono sottoscritti.

Dalla data di protocollazione decorre il termine per la conclusione del procedimento amministrativo di cui all'articolo 4 della legge provinciale 22 ottobre 1993, n. 17, e successive modifiche.

Nel caso di protocollazione di un documento cartaceo in ingresso, è facoltativo allegare alla registrazione di protocollo una scansione del documento e degli eventuali allegati. Si precisa che la scansione del documento cartaceo non sostituisce l'originale, il quale deve essere conservato negli archivi cartacei.

Nel caso di protocollazione di documenti informatici, il caricamento del documento e degli eventuali allegati nel registro di protocollo è obbligatorio sia in caso di protocollazione manuale che automatica e indipendentemente dal fatto che si tratti di un protocollo in ingresso, in uscita, interno o differito.
Il caricamento del documento informatico nel registro di protocollo è contestuale alla registrazione di protocollo.

I documenti informatici caricati nel registro di protocollo sono versati automaticamente nel sistema di conservazione digitale, che garantisce nel tempo l'integrità e la leggibilità dei documenti informatici e, se essi sono provvisti di firma digitale, la validità della firma.

3.2 Registro di protocollo

La protocollazione dei documenti è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal protocollo informatico.

Per la registrazione di protocollo sono obbligatorie le seguenti informazioni:

- numero di protocollo, generato automaticamente dal protocollo informatico e registrato in forma non modificabile;
- data di protocollo, assegnata automaticamente dal protocollo informatico e registrata in forma non modificabile;
- tipo di protocollo (ingresso, uscita, interno, differito);
- tipologia del documento ("default" o "fattura");
- indice di classificazione;
- mittente per i documenti in ingresso, o, in alternativa, destinatario o destinatari per i documenti interni ed esterni, registrati in forma non modificabile;
- oggetto del documento registrato in forma non modificabile (l'oggetto deve far comprendere il contenuto di un documento; evitare l'uso di abbreviazioni);
- fascicolo informatico;
- numero e descrizione sintetica degli allegati cartacei (se presenti);
- data di ingresso del documento per le protocollazioni differite;
- nome dell'autore/autrice della registrazione di protocollo, compilato automaticamente dal protocollo informatico e registrato in forma non modificabile;
- numero e data del protocollo del mittente (solo per documenti provenienti da enti pubblici);
- numero e data del protocollo di riferimento (se presente);
- mezzo di ricezione/spedizione.

Nel caso di protocollazione di documenti informatici sono altresì obbligatori:

- il caricamento del documento informatico e degli eventuali allegati informatici, memorizzati nel sistema di gestione documentale del protocollo informatico senza possibilità di modifica o cancellazione. Il formato del documento protocollato è di tipo PDF, PDF firmato digitalmente (PAdES) o P7M (CAdES);
- il calcolo dell'impronta del documento informatico (c.d. hash del file), eseguito dal protocollo informatico e memorizzato nel sistema di gestione documentale del protocollo informatico in forma non modificabile.

L'insieme delle registrazioni di protocollo costituisce il registro di protocollo.

3.3 Numero di protocollo e segnatura di protocollo

All'atto del salvataggio della registrazione di protocollo, il protocollo informatico genera automaticamente un numero progressivo, che è il numero di protocollo attribuito al documento, nonché la segnatura di protocollo.

Nel registro di protocollo della scuola la numerazione delle registrazioni di protocollo è unica e progressiva, senza distinzione tra i diversi tipi di protocollo. La numerazione ricomincia ogni anno solare. Nel corso dell'anno solare, ogni numero di protocollo è assegnato ad un solo documento; non è consentita l'attribuzione del medesimo numero di protocollo ad altri documenti, anche se strettamente correlati tra loro.

La segnatura di protocollo è composta dalla denominazione del registro di protocollo, dal numero di protocollo e dalla data di protocollo (es. 265100 IPC Brunico - Val Pusteria 2251 01.08.2016). La segnatura di protocollo consente l'individuazione univoca del documento.

Per quanto concerne i documenti informatici, l'associazione tra documento e segnatura è garantita dal protocollo informatico.
Per quanto concerne i documenti cartacei in ingresso, l'utente vi appone il timbro di protocollo di cui all'allegato n. 3 e lo compila con l'indicazione del numero di protocollo.

3.4 Fascicolo informatico

I documenti inerenti allo stesso procedimento amministrativo sono raccolti in un fascicolo informatico. Il fascicolo è l'unità minima di cui è composto l'archivio. Ogni fascicolo raccoglie documenti classificati in maniera omogenea; rappresenta un'eccezione il fascicolo digitale del personale.

I fascicoli informatici nel registro di protocollo sono creati dalla scuola. L'utente definisce l'indice di classificazione e la denominazione del fascicolo.
Ogni procedimento amministrativo ha un proprio indice di classificazione.
Il protocollo informatico assegna a ogni fascicolo un codice identificativo composto dalle seguenti informazioni: codice del registro di protocollo, indice di classificazione, anno di apertura del fascicolo e numero progressivo all'interno dell'indice di classificazione. La numerazione ricomincia ogni anno solare.
Il fascicolo informatico è assegnato in automatico alla scuola.

La chiusura del fascicolo è di competenza del responsabile del procedimento. La data di chiusura del fascicolo corrisponde alla data dell'ultimo documento in esso inserito.

Ogni fascicolo informatico contiene l'elenco dei documenti che esso comprende.

3.4.1 Tipologie di fascicolo

Oltre al fascicolo di procedimento amministrativo, che raccoglie una sequenza ordinata di atti finalizzati all'emanazione di un provvedimento finale, esistono le seguenti altre tipologie di fascicolo:

- il fascicolo di affare, che raccoglie i documenti relativi a un dato argomento ovvero a una competenza non procedimentalizzata, per i quali non è prevista l'adozione di un provvedimento finale (per es. organizzazione di un convegno o di un corso di formazione, insediamento di un gruppo di lavoro);
- il fascicolo di attività, che raccoglie documenti della stessa tipologia che vengono conservati per data (per es. raccolta dei pareri 2015, raccolta delle circolari 2015);
- il fascicolo di persona fisica, che raccoglie i documenti relativi a una persona fisica (per es. il fascicolo del personale);
- il fascicolo di persona giuridica, che raccoglie i documenti relativi a una persona giuridica (per es. associazioni, fondazioni, amministrazioni pubbliche).

3.5 Annullamento della registrazione di protocollo

Gli annullamenti devono essere autorizzati dal/la Dirigente scolastico/a.
Nell'autorizzazione all'annullamento (allegato n. 4) devono essere indicati il numero di protocollo e la data di protocollo della registrazione da annullare, nonché la motivazione dell'annullamento. Autorizzazioni cumulative sono ammesse solo qualora la motivazione dell'annullamento sia la stessa per tutte le registrazioni di protocollo indicate nell'autorizzazione.
Le autorizzazioni sono firmate digitalmente e caricate nel registro di protocollo.

La scheda di protocollo viene compilata come segue:

- tipo protocollo: interno;
- titolario: indice di classificazione della registrazione di protocollo da annullare;
- destinatario: Istituto Comprensivo Bassa Atresina;
- oggetto: "Autorizzazione all'annullamento della registrazione di protocollo IC Bassa Atesina 25900 e relativo numero di procollo prelevato singolarmente per l'annullamento di ciascuna procedura specifica.
- caricamento dell'autorizzazione firmata digitalmente.

Dopo aver protocollato l'autorizzazione all'annullamento, l'utente richiama la registrazione di protocollo da annullare e procede all'annullamento attraverso la selezione del pulsante "annullamento".

L'avvenuto annullamento di una registrazione di protocollo è riconoscibile da un'apposita dicitura o da un segno, generati in automatico. Le registrazioni di protocollo annullate possono essere visualizzate, ma non modificate. L'avvenuto annullamento di una registrazione di protocollo è tracciato in cronologia, unitamente al nome e al cognome dell'utente che lo ha eseguito, alla denominazione della scuola nonché alla data e all'ora dell'annullamento. Dalla sezione "altri dati" risultano gli estremi dell'autorizzazione all'annullamento.

3.6 Cronologia

A ogni registrazione di protocollo corrisponde una precisa cronologia, dalla quale risultano il nome e il cognome dell'autore/autrice della registrazione di protocollo, la denominazione della scuola, nonché la data e l'ora di protocollazione.
Ogni operazione (visualizzazione, modifica, annullamento) compiuta in relazione alle singole registrazioni di protocollo è tracciata nella corrispondente cronologia, unitamente al nome e al cognome dell'autore/autrice dell'intervento, alla denominazione della scuola, alla relativa data e ora. In caso di modifica di una registrazione di protocollo, in cronologia vengono tracciate anche le informazioni originarie. Non sono comunque ammesse modifiche relative ai dati registrati in forma non modificabile (numero di protocollo, data di protocollo, autore/autrice della registrazione di protocollo, assegnazione della registrazione di protocollo alla scuola, oggetto, mittente/destinatario, documento principale e allegati caricati).
La scheda della cronologia è legata indissolubilmente alla corrispondente registrazione di protocollo e i dati in essa contenuti non possono essere cancellati.
Per il calcolo della data e dell'ora della protocollazione, nonché di tutti i successivi interventi sulle singole registrazioni di protocollo, il protocollo informatico utilizza l'orario di sistema dei server, sincronizzati tra loro tramite il protocollo NTP (Network Time Protocol), e collegati ad un elenco di Server NTP ufficiali.

3.7 Registro giornaliero di protocollo

A fine giornata, il protocollo informatico genera in automatico il registro giornaliero di protocollo, il quale viene trasmesso, entro la giornata lavorativa successiva, al sistema di conservazione digitale al fine di garantirne l'immodificabilità e validità legale nel tempo, così come previsto dall'articolo 7, comma 5, del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 in materia di protocollo informatico. Non è consentita la stampa su carta del registro giornaliero di protocollo, in quanto la versione digitale è l'unica avente valore legale.
Per esigenze di consultazione, gli utenti possono generare in autonomia esportazioni delle registrazioni di protocollo in base ai criteri di ricerca impostati.

3.8 Registro di emergenza

Nell'impossibilità di utilizzare il registro di protocollo per un lasso di tempo superiore alle 48 ore, il/la Dirigente scolastico/a autorizza la protocollazione sul registro di emergenza (allegato n. 5) di cui all'articolo 63 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modifiche, e ai sensi dell'articolo 5, comma 2, lettera q) del decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 in materia di protocollo informatico.
Il numero di protocollo assegnato ai documenti protocollati nel registro di emergenza è preceduto dal codice "E" (per es. E1, E2, ecc.).
Le protocollazioni effettuate nel registro di emergenza vanno prontamente inserite nel registro di protocollo al ripristino delle sue funzionalità.

3.9 Descrizione funzionale del protocollo informatico

Per la descrizione funzionale del protocollo informatico si rimanda al Manuale utente (allegato n. 6).

4. Protocollo in ingresso

4.1 Protocollo in ingresso

La protocollazione dei documenti in ingresso è effettuata presso le sedi di protocollo entro la giornata di arrivo. Le buste della posta in ingresso vanno conservate in tutti i casi in cui la data di spedizione assuma rilevanza giuridica. La busta va scansionata e annotata nel registro di protocollo come allegato, unitamente alla data e all'ora risultanti dal timbro postale.

La corrispondenza riportante la dicitura "riservata", "personale" o indicazioni analoghe non devono essere aperte, in quanto considerate corrispondenza riservata.

I documenti pervenuti via fax vanno protocollati. Nel caso in cui alla trasmissione via fax segua l'invio del documento per posta, non si procede a nuova protocollazione, a meno che il documento non abbia subito modifiche.

La protocollazione dei messaggi di posta elettronica avviene direttamente attraverso il protocollo informatico, come illustrato nel Manuale utente di cui all'allegato n. 6; ciò avviene tramite il caricamento automatico del testo del messaggio, degli allegati e del messaggio nel suo formato originale nel registro di protocollo.

Nel caso di protocollazione di un messaggio di interoperabilità, il documento principale e gli eventuali allegati sono caricati in automatico nelle rispettive sezioni della scheda di protocollo.

Nel caso di protocollazione automatica, anche il documento informatico e gli eventuali allegati sono caricati nel registro di protocollo in automatico.

Nel caso di consegna del documento informatico su supporti di memoria esterni o in cloud, l'utente deve caricare il documento nel registro di protocollo contestualmente alla protocollazione.

La verifica circa la validità della firma digitale in formato CAdES (file con estensione .p7m) avviene attraverso il protocollo informatico. Una volta caricato il documento e ancora prima del suo salvataggio, il protocollo informatico dà immediatamente un messaggio relativo alla validità della firma e chiede di procedere alla verifica del certificato. Se entrambe le verifiche danno esito positivo, la firma digitale è valida. La verifica circa la validità della firma digitale in formato PAdES (file con estensione .pdf) deve invece avvenire utilizzando il programma "DIKE".

4.2 Rilascio delle ricevute

Se il mittente o una persona incaricata consegna personalmente un documento cartaceo e chiede una ricevuta che ne attesti l'avvenuta consegna, il personale è tenuto a rilasciare gratuitamente una fotocopia della prima pagina del documento protocollato, su cui è apposta la segnatura di protocollo.
Se un documento informatico viene consegnato su un supporto di memoria esterno oppure se viene ricevuto tramite posta elettronica o tramite cloud, e qualora venga richiesta una ricevuta di consegna, il personale è tenuto ad inviare la segnatura di protocollo nel formato XML all'indirizzo di posta elettronica indicato dal richiedente oppure a salvarla nel supporto di memoria esterno.

Nel caso di invio di documenti informatici tramite i servizi online dell'Amministrazione provinciale (eGov), la segnatura di protocollo viene comunicata al richiedente in una o più delle seguenti modalità:

- visualizzazione all'interno del servizio online subito dopo l'avvenuta protocollazione;
- deposito all'interno dell'area personale eGov;
- invio automatico via posta elettronica.

4.3 Ricezione dei documenti informatici

La ricezione dei documenti informatici avviene tramite:

- la casella di posta elettronica certificata (PEC) della scuola;
- la casella istituzionale di posta elettronica ordinaria della scuola;
- le caselle di posta elettronica specifiche per singoli procedimenti amministrativi;
- i servizi online dell'Amministrazione provinciale (eGov);
- altri servizi digitali (per es. cooperazione applicativa);
- supporti di memoria esterni o cloud.

4.4 Validità delle istanze, dichiarazioni e segnalazioni presentate per via elettronica

Le istanze, le dichiarazioni e le segnalazioni presentate alla scuola per via elettronica sono valide esclusivamente:

- se sono sottoscritte con firma digitale;
- oppure se sono trasmesse tramite posta elettronica certificata (PEC) e sottoscritte con firma digitale;
- oppure se l'identificazione dell'utente avviene (a seconda del livello minimo di sicurezza richiesto) mediante:
    - la Carta Nazionale dei Servizi (CNS);
    - l'Identità Digitale Alto Adige;
    - il Sistema Pubblico per la gestione dell'Identità Digitale (SPID);
- oppure se sono sottoscritte e presentate unitamente alla copia del documento d'identità, limitatamente ai casi in cui non sia disponibile il corrispondente servizio online.

4.5 Presentazione di istanze, dichiarazioni e segnalazioni attraverso i servizi online

La presentazione di istanze, dichiarazioni e segnalazioni attraverso i servizi online dell'Amministrazione provinciale (es. servizio di iscrizione online - IOLE) avviene con la seguente procedura:

- identificazione del richiedente;
- inserimento dei dati in modo interattivo e guidato;
- assolvimento dell'imposta di bollo elettronica, se dovuta;
- trasmissione del documento informatico e del rispettivo file XML, generati sulla base dei dati inseriti;
- protocollazione e fascicolazione automatica del documento e del file XML trasmessi;
- comunicazione dell'esito della registrazione di protocollo come descritto al paragrafo 4.2.

5. Protocollo in uscita

5.1 Protocollo in uscita:

Per quanto concerne la formazione e la sottoscrizione dei documenti informatici si rimanda al capitolo 2 "Documento informatico".

Sono protocollati in uscita i documenti redatti dalla scuola e diretti a destinatari esterni alla scuola stessa.
La protocollazione dei documenti in uscita è effettuata subito dopo la loro sottoscrizione. Si ricorda che è obbligatorio il caricamento dei documenti informatici nel registro di protocollo.

5.2 Trasmissione dei documenti

5.2.1 Trasmissione dei documenti a cittadini e cittadine

Qualora il cittadino/la cittadina abbia indicato alla scuola un proprio indirizzo di posta elettronica certificata (PEC) quale suo domicilio digitale, i documenti a lui/lei indirizzati vengono trasmessi esclusivamente a tale

indirizzo. In tutta la modulistica della scuola deve essere previsto un apposito campo per l'indicazione del domicilio digitale.
La trasmissione del documento informatico a mezzo posta elettronica certificata (PEC) equivale alla notificazione a mezzo posta (articolo 48 del CAD), salvo che la legge disponga diversamente.

In assenza del domicilio digitale, al cittadino/alla cittadina è inviata una copia cartacea tratta dal documento informatico originale, la quale riporta, oltre alla segnatura di protocollo, i dati di riferimento del certificato impiegato ai fini della sottoscrizione del documento e un'annotazione relativa alla conservazione del documento originale a norma di legge. Nel caso in cui sussista un obbligo di notifica, la copia cartacea è inviata a mezzo raccomandata con avviso di ricevimento (RAR), altrimenti è inviata per posta ordinaria.
La copia cartacea viene realizzata tramite un apposito applicativo.

Nel caso di servizi online è altresì previsto il deposito dei documenti nell'area personale eGov.

5.2.2 Trasmissione dei documenti al personale provinciale

I documenti e la documentazione concernenti il rapporto di lavoro del personale dirigente e docente delle scuole a carattere statale e del personale provinciale sono depositati, di norma, nel fascicolo digitale dei singoli dipendenti e non sono più trasmessi a mezzo posta cartacea.
Il fascicolo digitale del personale dirigente, docente e ispettivo delle scuole a carattere statale è gestito dalla Ripartizione Personale e dalle rispettive Intendenze scolastiche, mentre quello del personale provinciale è gestito dalla Ripartizione Personale.

5.2.3 Trasmissione dei documenti alle imprese

La comunicazione tra la scuola e le imprese avviene esclusivamente in forma elettronica attraverso:

- piattaforme dedicate (per es. SUAP);
- posta elettronica certificata (PEC).

I messaggi di posta elettronica certificata devono essere inviati agli indirizzi risultanti dall'INI-PEC, l'Indice Nazionale degli Indirizzi di posta elettronica certificata istituito dal Ministero dello Sviluppo Economico (http://www.inipec.gov.it).

5.2.4 Trasmissione dei documenti tra pubbliche amministrazioni

La trasmissione dei documenti tra le pubbliche amministrazioni (ad es. tra la scuola e l'Amministrazione provinciale o tra la scuola e il Comune) avviene tramite:

- posta elettronica ordinaria;
- posta elettronica certificata;
- interoperabilità tra sistemi di protocollo informatico;
- cooperazione applicativa.

Tra le pubbliche amministrazioni non è ammessa la trasmissione di documenti a mezzo fax.

In tutti i casi di cui sopra, ai fini della trasmissione dei documenti tramite posta elettronica, l'utente ricorre alla funzione di interoperabilità del protocollo informatico (cfr. capitolo 10 del Manuale utente di cui all'allegato n. 6). Al destinatario/alla destinataria viene inviato un messaggio di posta elettronica, denominato "protocollo di interoperabilità", contenente il documento informatico, eventuali allegati e un file "segnatura.xml" contenente la segnatura di protocollo e i rispettivi metadati.

5.3 Protocollazione di messaggi di posta elettronica in uscita

La protocollazione di messaggi di posta elettronica ordinaria e certificata in uscita deve essere effettuata solo se i messaggi di posta elettronica non contengono documenti già protocollati nel registro di protocollo della scuola, perché altrimenti si avrebbe una doppia protocollazione del documento.

5.4 Spedizione di documenti non soggetti a protocollazione

La spedizione di documenti o comunicazioni non soggetti a protocollazione avviene di norma tramite le caselle di posta elettronica nominative (ad es. casella di posta elettronica di un assistente di segreteria oppure casella di posta elettronica di un docente).

6. Protocollo interno

Per quanto concerne la formazione e la sottoscrizione dei documenti informatici, si rimanda al capitolo 2 "Documento informatico".

Le comunicazioni interne di carattere informale non sono soggette a protocollazione e la loro trasmissione avviene tramite le caselle di posta elettronica nominative.

6.1 Competenza e conoscenza

Quando un documento è indirizzato sia a destinatari esterni alla scuola, sia a destinatari interni alla stessa, ai fini della scelta del "tipo protocollo" va osservato quanto segue:

- la competenza prevale sulla conoscenza;
- il destinatario esterno prevale sul destinatario interno.

Se un documento è indirizzato a un destinatario interno per competenza e a un destinatario esterno per conoscenza, l'utente seleziona il tipo protocollo "interno", in quanto la competenza prevale sulla conoscenza.
Se un documento è indirizzato a un destinatario esterno e a un destinatario interno, ed entrambi i destinatari sono destinatari per competenza, l'utente seleziona il tipo protocollo "uscita", in quanto il destinatario esterno prevale sul destinatario interno.
Se un documento è indirizzato a un destinatario esterno per competenza e a un destinatario interno per conoscenza, l'utente seleziona il tipo protocollo "uscita", in quanto il destinatario esterno prevale sul destinatario interno e la competenza prevale sulla conoscenza.

7. Protocollo differito

La protocollazione può essere differita solo in caso di temporaneo ed eccezionale carico di lavoro che non permetta di protocollare i documenti in giornata. La data di ingresso dei documenti è annotata nel registro di protocollo.
I documenti cartacei la cui protocollazione viene differita devono essere datati e siglati dalla persona che li riceve.

Nel caso di protocollazione automatica effettuata da sistemi informatici, qualora per problemi tecnici non sia possibile eseguire la protocollazione entro la giornata di arrivo, al ripristino delle funzionalità il sistema provvederà ad effettuare una protocollazione differita.
Quando la data di ingresso dei messaggi di posta elettronica è anteriore alla data di protocollo, il protocollo informatico compila la scheda del "protocollo differito" in automatico.

8. Registrazione particolare

Sono soggetti a registrazione particolare:

a) le delibere del Consiglio di Istituto;
b) i decreti del/la Dirigente Scolastico/a;
c) le delibere del Collegio dei docenti;
d) i diplomi;
e) i certificati rilasciati dalla scuola (di iscrizione, di servizio, …)
f) …

Questi documenti sono sottoscritti con firma digitale. Per la registrazione di tali atti saranno predisposte applicazioni che gestiscono la fase di redazione, garantiscono la numerazione ininterrotta in ordine progressivo per anno solare, salvano i documenti nel sistema di gestione documentale e li versano automaticamente nel sistema di conservazione digitale dell'Amministrazione provinciale.

9. Fattura elettronica

Ai fini della ricezione delle fatture elettroniche, alla scuola è assegnato un "codice univoco ufficio" risultante dall'Indice PA (http://www.indicepa.gov.it). Il codice univoco ufficio deve essere attivato dalla persona indicata come referente per il registro di protocollo 25900 IC Bassa Atesina.

10. Formati ammessi per i documenti informatici in ingresso

La scuola accetta esclusivamente i formati di file elencati nella sezione "Formati di file ammessi" del sito web della scuola, ma non è tenuta a rispondere utilizzando lo stesso formato.
L'accettazione di file non conformi ai formati di file ammessi o di file contenenti codice eseguibile o macroistruzioni deve essere preventivamente concordata ed è ammessa solo in casi eccezionali.

11. Titolario

Il titolario unico delle scuole è pubblicato nell'allegato n. 7.
Eventuali modifiche al titolario possono essere effettuate solo con decreto del Direttore generale/della Direttrice generale.

12. Archivio

I documenti informatici devono essere caricati nel registro di protocollo. Il sistema di conservazione digitale costituisce l'archivio di deposito dei documenti informatici. Una volta versati nel sistema di conservazione digitale, i documenti informatici restano comunque visibili nel registro di protocollo.
Decorsi i tempi di conservazione, i documenti vengono sottoposti ad una procedura di selezione, che consiste nell'individuazione dei documenti da scartare e dei documenti da destinare alla conservazione permanente. Le decisioni in merito competono alla commissione di sorveglianza e scarto della scuola.
Lo scarto formale consiste nell'eliminazione dei documenti informatici. I documenti informatici destinati alla conservazione permanente permangono nel sistema di conservazione digitale.

13. Conservazione dei documenti informatici

I documenti informatici soggetti a conservazione sono automaticamente versati nel sistema di conservazione digitale tramite interoperabilità tra sistemi, secondo le regole stabilite per ciascuna tipologia di documento.

14. Abilitazione all'accesso al protocollo informatico

14.1 Accesso

Hanno accesso alle registrazioni di protocollo della scuola gli utenti assegnati ai corrispondenti nodi dell'organigramma del protocollo informatico.
Il/La Dirigente scolastico/a ha accesso a tutte le registrazioni di protocollo del registro della scuola.

14.2 Key-User

La scuola ha un key-user, nominato dal/la Dirigente scolastico/a.

Il key-user:

- assegna gli utenti al rispettivo nodo di organigramma;
- attiva le abilitazioni alla protocollazione.

Ogni key-user accede unicamente all'organigramma relativo al rispettivo dipartimento o alla rispettiva ripartizione.

Le attività di cui sopra sono svolte per mezzo del programma di gestione per key-user.

14.3 Amministratore di registro

Informatica Alto Adige S.p.A. assolve ai compiti di amministratore del registro di protocollo della scuola.

L'amministratore del registro di protocollo:

- gestisce le utenze key-user;
- gestisce le tabelle di configurazione del sistema;
- effettua l'importazione dei registri di emergenza nel registro di protocollo della scuola.

Le attività di cui sopra sono svolte per mezzo del programma di gestione dell'amministratore di registro.

14.4 Accesso da applicazioni

I servizi di protocollo informatico sono disponibili per la cooperazione applicativa. A tal fine, ogni applicazione che necessita di un accesso al protocollo accede ai servizi di cooperazione applicativa mediante utenze di servizio o utenze nominali. Anche in questi casi il controllo degli accessi viene gestito secondo i criteri citati nel presente capitolo.

15. Piano di sicurezza

Nel maggio 2011 Informatica Alto Adige S.p.A., ente strumentale in house della Provincia autonoma di Bolzano, e la Ripartizione Informatica della Provincia hanno inaugurato un Data Center comune, con sede a Bolzano, che ha la funzione di ospitare l'infrastruttura informatica delle due entità.
Con deliberazione n. 1048 dell'11 luglio 2011 la Giunta provinciale ha deciso di riorganizzare l'intero settore informatico della Provincia, trasferendone la parte operativa a Informatica Alto Adige S.p.A. e la guida strategica alla Ripartizione Informatica.
Informatica Alto Adige S.p.A. è quindi diventata il braccio operativo della Provincia e delle istituzioni scolastiche per quanto riguarda l'informatica e ha ora in carico la gestione dell'intera infrastruttura del Data Center e di tutti i servizi informatici offerti dalla Ripartizione Informatica della Provincia alle altre Ripartizioni.
Il rapporto tra Provincia autonoma di Bolzano e Informatica Alto Adige S.p.A. è disciplinato nell'Accordo quadro ai sensi della legge provinciale 8 novembre 1982, n. 33.

Informatica Alto Adige S.p.A. è in possesso delle seguenti certificazioni:

- Certificazione di qualità UNI EN ISO 9001:2008 "Sviluppo ed erogazione di servizi nel settore dell'information technology"
- Certificazione di sicurezza UNI CEI ISO/IEC 27001:2013 per il Sistema di Gestione della Sicurezza delle Informazioni (ISMS – Information Security Management System) - "Sviluppo ed erogazione di servizi nel settore dell'information technology".

15.1 Sicurezza dei sistemi informatici

Informatica Alto Adige S.p.A. ha introdotto e applica un sistema di gestione della sicurezza delle informazioni in relazione allo sviluppo e all'erogazione di servizi nel settore dell'information technology, così come certificato dallo standard adottato ISO/IEC 27001:2013.

15.2 Sicurezza nella conservazione dei documenti

Il sistema adottato per garantire la sicurezza nella conservazione dei documenti è descritto nell'allegato n. 8.

15.3 Politiche di sicurezza della scuola

Sul sito della scuola sono pubblicati i Codici di comportamento del personale e dei dirigenti della Provincia (Deliberazione della Giunta provinciale n. 938 del 29 luglio 2014) e del personale dirigente e direttivo delle scuole a carattere statale (DPR n. 62/2013), che definiscono gli obblighi di servizio e di comportamento del personale e, ove possibile, del personale esterno che lavora a vario titolo per la scuola (allegati n. 9a e 9b).

Secondo quanto indicato dal Garante della Privacy nelle "Linee guida del Garante per posta elettronica e internet" (G.U. n. 58 del 10 marzo 2007), è stato approvato il "Disciplinare organizzativo per l'utilizzo dei servizi informatici, in particolare di internet e della posta elettronica, da parte degli uffici provinciali e dell'amministrazione scolastica" (allegato n. 10), pubblicato con la relativa circolare (allegato n. 11).

Principio base del disciplinare è limitare l'uso di tutti gli strumenti IT adottati dalla scuola, sia che si tratti di software che di hardware, ad esigenze esclusivamente di tipo lavorativo, vietandone quindi qualunque uso a scopo privato.
Il disciplinare contiene regole sull'installazione di software, sull'uso di internet e della posta elettronica nonché sul rispetto della proprietà intellettuale e delle licenze.
Con questo disciplinare si persegue l'obiettivo di aumentare la sicurezza di tutti i dati e delle informazioni gestiti tramite servizi informatici e di impedirne l'uso per scopi privati. Ne consegue che, se l'organizzazione del lavoro lo richiede, il/la Dirigente scolastico/a può accedere per esempio alla casella di posta di un collaboratore, anche in sua assenza, senza essere tenuto a chiedergli il permesso.
Il personale tecnico può, in determinate condizioni, accedere ai file di dati o di navigazione in internet, se ciò fosse necessario per risolvere un problema tecnico, per esempio in caso di memoria insufficiente o di lentezza della rete. Lo scopo non è assolutamente quello di controllare il collaboratore nella sua attività lavorativa, ma di poter effettuare controlli di tipo tecnico, senza per questo violare i diritti di riservatezza.
Negli anni, anche in osservanza delle norme divenute più stringenti e delle best practice per la sicurezza, sono stati adottati vari regolamenti e policy finalizzati a soddisfare i più elevati requisiti richiesti in termini di sicurezza fisica e logica – ora implementati dal gestore del servizio informatico, Informatica Alto Adige S.p.A. – in parte anche in materia di sicurezza organizzativa; questi regolamenti e queste policy sono ovviamente rivolti al personale dell'Amministrazione provinciale.
A titolo esemplificativo e non esaustivo basti menzionare la circolare del Direttore generale del 6 dicembre 2001 sull'uso delle credenziali informatiche, in particolare della password (allegato n. 12), in rispondenza alla Policy di gestione dell'account (allegato n. 13).

16. Disposizioni finali

Per quanto non espressamente previsto dal presente Manuale trova applicazione la normativa vigente in materia.

ALLEGATI (i presenti allegati non sono parte integrante della delibera bensì del manuale stesso).

Allegato n. 1 Normativa di riferimento
Allegato n. 2 Formati di file adottati dall'Amministrazione provinciale

Allegato n. 3 Timbro di protocollo dell'Amministrazione provinciale

Allegato n. 4 Modulo per annullamento

Allegato n. 5 Registro di emergenza

Allegato n. 6 Manuale utente

Allegato n. 7 Titolario dell'Amministrazione provinciale

Allegato n. 8 Sicurezza nella conservazione dei documenti

Allegato n. 9a e 9b Codice di comportamento del personale e dei dirigenti della Provincia e del personale docente e dirigente delle scuole

Allegato n. 10 Disciplinare organizzativo per l'utilizzo dei servizi informatici

Allegato n. 11 Circolare sul Disciplinare organizzativo per l'utilizzo dei servizi informatici

Allegato n. 12 Circolare sulla Protezione dell'accesso al sistema informatico

Allegato n. 13 Policy gestione account