ALLEGATO 4

INFORMATIVA E ISTRUZIONI OPERATIVE PER LA PROTEZIONE DEI DATI PERSONALI E LA SICUREZZA INFORMATICA NELLO SVOLGIMENTO DEL LAVORO AGILE

1. Oggetto e finalità

1. Il presente documento costituisce parte integrante del **Regolamento per la disciplina del lavoro agile del personale ATA** dell'Istituzione scolastica e contiene le disposizioni e le istruzioni operative cui il dipendente è tenuto ad attenersi nello svolgimento della prestazione lavorativa in modalità agile.
2. Le presenti disposizioni hanno la finalità di:
   a) garantire la protezione dei dati personali trattati nello svolgimento dell'attività lavorativa;
   b) assicurare la riservatezza delle informazioni e dei documenti dell'Istituzione scolastica;
   c) prevenire accessi non autorizzati ai sistemi informativi;
   d) garantire l'integrità, la disponibilità e la sicurezza dei dati;
   e) ridurre il rischio di perdita, distruzione, alterazione, divulgazione o trattamento non autorizzato dei dati;
   f) assicurare un utilizzo corretto e sicuro delle apparecchiature e dei servizi informatici messi a disposizione dall'Istituzione scolastica.
3. Il dipendente è tenuto a conoscere e rispettare, oltre alle presenti istruzioni, le ulteriori disposizioni dell'Istituzione scolastica in materia di protezione dei dati personali, sicurezza informatica, utilizzo degli strumenti informatici, posta elettronica, accesso alla rete e gestione delle credenziali.

2. Quadro normativo di riferimento

1. Il trattamento dei dati personali effettuato nell'ambito della prestazione lavorativa in modalità agile è soggetto alla normativa vigente in materia di protezione dei dati personali e, in particolare:

a) al Regolamento (UE) 2016/679 (GDPR);
b) al decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101;
c) alla normativa nazionale vigente in materia di protezione dei dati personali;
d) alla normativa in materia di lavoro agile;
e) alle disposizioni del CCNL applicabile;
f) alle disposizioni interne dell'Istituzione scolastica;
g) alle istruzioni impartite dal Titolare del trattamento e dai soggetti competenti in materia di protezione dei dati e sicurezza informatica.

2. Il trattamento dei dati personali nello svolgimento del lavoro agile deve essere effettuato nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.
3. Il dipendente, nello svolgimento delle proprie mansioni, opera esclusivamente nell'ambito delle autorizzazioni e delle competenze attribuitegli dall'Istituzione scolastica.

3. Ruolo del dipendente nel trattamento dei dati

1. Il dipendente, in relazione alle mansioni assegnate, può essere autorizzato al trattamento dei dati personali per conto dell'Istituzione scolastica.
2. Il dipendente può accedere esclusivamente ai dati, alle informazioni, ai fascicoli, alle banche dati, ai gestionali e alle risorse informatiche necessari allo svolgimento delle proprie mansioni.
3. È vietato accedere a dati, documenti o informazioni per motivi estranei allo svolgimento dell'attività lavorativa, anche qualora tecnicamente accessibili.
4. Il dipendente è tenuto a rispettare il principio di riservatezza anche nei confronti di altri dipendenti dell'Istituzione scolastica che non siano autorizzati ad accedere alle medesime informazioni.
5. L'obbligo di riservatezza permane anche successivamente alla cessazione, per qualsiasi motivo, del rapporto di lavoro o dell'autorizzazione al trattamento.

Il Garante ha recentemente ribadito che i dati dei lavoratori e gli altri dati trattati nell'ambito dell'organizzazione non devono essere resi conoscibili a soggetti privi di una specifica necessità connessa alle funzioni esercitate.

4. Principio di minimizzazione

1. Il dipendente deve trattare esclusivamente i dati personali necessari allo svolgimento delle attività assegnate.
2. Non devono essere effettuate copie, download, stampe, esportazioni o trasferimenti di dati personali che non siano necessari per l'attività lavorativa.

3. Qualora una determinata attività possa essere svolta utilizzando dati anonimizzati, pseudonimizzati o comunque ridotti al minimo necessario, il dipendente deve utilizzare, ove previsto dall'organizzazione dell'Istituzione scolastica, la modalità che comporti il minor trattamento di dati personali.
4. È vietato conservare sul dispositivo utilizzato per il lavoro agile copie di dati personali oltre il tempo strettamente necessario allo svolgimento dell'attività.

5. Luogo di svolgimento della prestazione

1. Il dipendente è tenuto a scegliere un luogo di svolgimento della prestazione che consenta di garantire adeguate condizioni di riservatezza e sicurezza.
2. Durante lo svolgimento della prestazione il dipendente deve adottare tutte le cautele necessarie affinché:
   a) persone estranee all'attività lavorativa non possano vedere lo schermo;
   b) persone estranee non possano ascoltare conversazioni o comunicazioni contenenti informazioni riservate;
   c) documenti cartacei non siano lasciati incustoditi;
   d) apparecchiature e dispositivi non siano accessibili a terzi;
   e) le credenziali di accesso non siano visualizzabili o utilizzabili da altre persone.
3. Il dipendente deve evitare, ove possibile, lo svolgimento di attività contenenti dati personali in luoghi pubblici o caratterizzati da elevato affollamento.
4. È vietato lasciare incustoditi documenti, dispositivi o supporti contenenti dati personali.

6. Utilizzo dei dispositivi dell'Istituzione scolastica

1. Le apparecchiature informatiche eventualmente messe a disposizione dall'Istituzione scolastica devono essere utilizzate esclusivamente secondo le finalità e le modalità previste dall'Amministrazione.
2. Il dipendente deve:
   a) custodire con cura il dispositivo;
   b) non consentirne l'utilizzo a familiari, conoscenti o altri soggetti;
   c) non installare software non autorizzati;
   d) non modificare le configurazioni di sicurezza;
   e) non disattivare antivirus, firewall o altri sistemi di protezione;
   f) non utilizzare dispositivi esterni non autorizzati;
   g) mantenere aggiornato il dispositivo secondo le procedure predisposte dall'Istituzione scolastica;
   h) comunicare tempestivamente eventuali anomalie.
3. Il dispositivo deve essere protetto mediante le misure di autenticazione e sicurezza predisposte dall'Istituzione scolastica.
4. Al termine della prestazione il dispositivo deve essere spento o bloccato secondo le procedure interne, evitando che terzi possano accedere alle informazioni presenti.

7. Utilizzo di dispositivi personali

1. L'utilizzo di dispositivi personali per lo svolgimento del lavoro agile è consentito esclusivamente nei casi e alle condizioni previste dalla contrattazione integrativa di istituto e dall'accordo individuale.
2. Il dipendente che utilizza un dispositivo personale è tenuto ad adottare tutte le misure necessarie a garantire la sicurezza dei dati e delle informazioni dell'Istituzione scolastica.
3. Il dispositivo personale utilizzato per il lavoro agile deve essere dotato, ove tecnicamente disponibile e necessario:
   a) di sistema operativo aggiornato;
   b) di sistemi di protezione da malware;
   c) di password o altro sistema di autenticazione;
   d) di blocco automatico dello schermo;
   e) di sistemi di cifratura, ove richiesti dall'Istituzione scolastica;
   f) di connessione sicura.
4. È vietato consentire a familiari o terzi l'utilizzo del dispositivo mentre sono aperte sessioni o applicazioni contenenti dati dell'Istituzione scolastica.
5. Il dipendente deve mantenere separati, per quanto tecnicamente possibile, i dati e le attività personali da quelli lavorativi.
6. L'Istituzione scolastica può stabilire che determinate attività o trattamenti non possano essere effettuati mediante dispositivi personali.

8. Credenziali di autenticazione

1. Le credenziali di accesso ai sistemi dell'Istituzione scolastica sono personali e non possono essere cedute, comunicate o rese disponibili a terzi.
2. Il dipendente deve:
   a) utilizzare password adeguatamente robuste;
   b) non annotare le password in luoghi accessibili ad altre persone;
   c) non utilizzare la medesima password, ove possibile, per servizi personali e sistemi istituzionali;
   d) non comunicare le credenziali tramite e-mail, messaggistica o telefono, salvo procedure di

assistenza espressamente previste;
e) modificare la password quando richiesto dall'Amministrazione o dal sistema;
f) segnalare immediatamente eventuali sospetti di compromissione delle credenziali.

3. Qualora sia prevista l'autenticazione a più fattori, il dipendente è tenuto a utilizzarla secondo le procedure dell'Istituzione scolastica.

9. Posta elettronica istituzionale

1. La posta elettronica istituzionale deve essere utilizzata esclusivamente secondo le finalità connesse all'attività lavorativa.
2. Il dipendente deve prestare particolare attenzione:
   a) ai messaggi provenienti da mittenti sconosciuti;
   b) agli allegati inattesi;
   c) ai collegamenti contenuti nelle e-mail;
   d) alle richieste di credenziali o dati personali;
   e) alle comunicazioni che presentino caratteristiche anomale o sospette.
3. È vietato inoltrare a caselle di posta elettronica personali documenti contenenti dati personali o informazioni riservate dell'Istituzione scolastica, salvo specifica autorizzazione e nei casi in cui ciò sia indispensabile per lo svolgimento dell'attività.
4. È vietato utilizzare account personali per sostituire ordinariamente gli strumenti istituzionali di comunicazione.
5. Il dipendente deve prestare particolare attenzione all'indirizzo del destinatario prima dell'invio di comunicazioni contenenti dati personali.
6. In caso di invio errato di una comunicazione contenente dati personali, il dipendente deve informare tempestivamente l'Istituzione scolastica secondo le procedure interne per la gestione degli incidenti di sicurezza.

10. Accesso ai sistemi informativi

1. L'accesso ai sistemi informativi dell'Istituzione scolastica deve avvenire esclusivamente attraverso le modalità autorizzate.
2. Il dipendente non deve:
   a) aggirare sistemi di autenticazione;
   b) utilizzare credenziali di altri utenti;
   c) modificare o disattivare sistemi di sicurezza;
   d) utilizzare software o strumenti destinati ad eludere le misure di protezione;
   e) effettuare accessi a banche dati o cartelle non necessari allo svolgimento delle proprie mansioni.
3. Qualora l'accesso da remoto richieda sistemi specifici, quali VPN, autenticazione multifattore o altri strumenti di sicurezza, il dipendente è tenuto a utilizzare esclusivamente quelli messi a disposizione o autorizzati dall'Istituzione scolastica.

11. Connessione Internet

1. Per l'accesso ai sistemi dell'Istituzione scolastica devono essere utilizzate connessioni che offrano adeguati livelli di sicurezza.
2. Il dipendente deve evitare, per quanto possibile, l'utilizzo di reti Wi-Fi pubbliche o aperte per il trattamento di dati personali o per l'accesso ai sistemi istituzionali.
3. Qualora sia necessario utilizzare una rete non abituale, il dipendente deve adottare le misure di sicurezza indicate dall'Istituzione scolastica.
4. È vietato utilizzare reti o strumenti che presentino evidenti condizioni di insicurezza o che possano compromettere la riservatezza delle comunicazioni.

12. Documenti cartacei

1. Il trattamento di documenti cartacei contenenti dati personali al di fuori della sede scolastica deve essere limitato alle situazioni in cui sia effettivamente necessario e consentito dall'organizzazione dell'Istituzione scolastica.
2. I documenti cartacei devono essere:
   a) trasportati con modalità che ne impediscano lo smarrimento;
   b) custoditi in modo da impedirne l'accesso a soggetti non autorizzati;
   c) non lasciati incustoditi;
   d) protetti da consultazioni accidentali o non autorizzate.
3. È vietato lasciare documenti contenenti dati personali in automobile, in luoghi pubblici o in altri luoghi nei quali non sia possibile garantirne la sicurezza.
4. I documenti non più necessari devono essere restituiti all'Istituzione scolastica o distrutti secondo le procedure interne.
5. È vietato smaltire documenti contenenti dati personali nei normali rifiuti domestici.

13. Stampa e riproduzione dei documenti

1. La stampa di documenti contenenti dati personali deve essere limitata ai casi di effettiva necessità.
2. Il dipendente deve verificare che la stampante utilizzata sia in un luogo sicuro e non accessibile a terzi.

3. Le copie stampate devono essere custodite con le medesime cautele applicabili ai documenti originali.
4. Al termine della necessità di utilizzo, le copie devono essere restituite o distrutte secondo le procedure previste dall'Istituzione scolastica.

14. Supporti rimovibili e dispositivi esterni

1. L'utilizzo di chiavette USB, hard disk esterni, schede di memoria o altri supporti rimovibili per la memorizzazione o il trasferimento di dati dell'Istituzione scolastica è consentito esclusivamente quando autorizzato e necessario.
2. Ove previsto dalle misure di sicurezza dell'Istituzione scolastica, i supporti devono essere cifrati o protetti con modalità equivalenti.
3. È vietato utilizzare supporti personali non autorizzati per conservare dati personali dell'Istituzione scolastica.

15. Videoconferenze e comunicazioni a distanza

1. Le videoconferenze e le riunioni a distanza devono essere effettuate mediante le piattaforme autorizzate dall'Istituzione scolastica.
2. Il dipendente deve verificare che:
   a) il collegamento sia effettuato con l'account istituzionale, quando previsto;
   b) non siano presenti persone non autorizzate;
   c) lo schermo non sia visibile a terzi;
   d) eventuali documenti condivisi siano limitati a quelli necessari;
   e) la registrazione della riunione avvenga esclusivamente nei casi autorizzati.
3. È vietato registrare riunioni, conversazioni o videoconferenze relative all'attività lavorativa senza che ciò sia previsto o autorizzato.
4. Il dipendente deve prestare attenzione allo sfondo e all'ambiente circostante, evitando che siano accidentalmente visibili o udibili dati personali, documenti o informazioni riservate.

16. Telefonate e comunicazioni vocali

1. Le telefonate relative all'attività lavorativa devono essere effettuate in condizioni tali da evitare, per quanto possibile, l'ascolto da parte di soggetti estranei.
2. Particolare cautela deve essere adottata durante il trattamento o la comunicazione di:
   a) dati relativi agli alunni;
   b) dati relativi alla salute;
   c) dati relativi al personale;
   d) informazioni disciplinari;
   e) informazioni economiche;
   f) informazioni relative a procedimenti amministrativi;
   g) altre informazioni riservate.
3. In luoghi pubblici o comunque non riservati il dipendente deve evitare conversazioni contenenti dati personali o informazioni riservate.

17. Dati particolarmente delicati

1. Particolare attenzione deve essere prestata al trattamento di dati appartenenti a categorie particolari e di dati relativi a procedimenti o situazioni che richiedano elevati livelli di riservatezza.
2. In particolare, devono essere trattati con particolare cautela i dati relativi:
   a) alla salute;
   b) alla disabilità;
   c) a situazioni familiari;
   d) a procedimenti disciplinari;
   e) a condizioni economiche;
   f) a minori;
   g) a procedimenti amministrativi riservati.
3. Il dipendente deve limitare il trattamento a quanto strettamente necessario per lo svolgimento delle mansioni assegnate.
4. Il dipendente non deve acquisire, conservare o comunicare informazioni relative alla salute o ad altre categorie particolari di dati quando tali informazioni non siano necessarie allo svolgimento della specifica attività lavorativa.

18. Conservazione dei dati

1. I dati e i documenti devono essere conservati esclusivamente nei sistemi e negli archivi individuati dall'Istituzione scolastica.
2. È vietato utilizzare servizi personali di cloud storage, posta elettronica, messaggistica o piattaforme di condivisione per conservare dati dell'Istituzione scolastica, salvo espressa autorizzazione.
3. I file contenenti dati personali devono essere eliminati dal dispositivo utilizzato per il lavoro agile quando non siano più necessari e quando ciò sia compatibile con le procedure di conservazione dell'Istituzione scolastica.
4. La cancellazione dei file dal dispositivo personale non sostituisce le procedure istituzionali di conservazione e archiviazione dei documenti.

19. Divieto di utilizzo di strumenti personali non autorizzati

1. È vietato utilizzare applicazioni, piattaforme, servizi di messaggistica, sistemi di archiviazione o strumenti di intelligenza artificiale non autorizzati dall'Istituzione scolastica per trattare dati personali o informazioni riservate dell'Amministrazione.
2. In particolare, il dipendente non deve inserire dati personali, documenti scolastici, informazioni relative agli alunni, alle famiglie o al personale in servizi esterni non espressamente autorizzati.
3. L'eventuale utilizzo di strumenti tecnologici innovativi per attività lavorative deve essere preventivamente valutato e autorizzato dall'Istituzione scolastica, secondo le procedure interne.

20. Sicurezza fisica dei dispositivi

1. Il dipendente deve adottare misure ragionevoli per impedire il furto, lo smarrimento o l'accesso non autorizzato ai dispositivi utilizzati per il lavoro agile.
2. In caso di spostamento con un dispositivo dell'Istituzione scolastica, il dipendente deve evitare di lasciarlo incustodito.
3. Qualora il dispositivo debba essere lasciato temporaneamente in un veicolo, deve essere collocato in condizioni tali da non risultare visibile dall'esterno e deve essere adottata ogni ulteriore misura ragionevole di sicurezza.
4. In caso di furto o smarrimento di dispositivi o supporti contenenti dati dell'Istituzione scolastica, il dipendente deve darne comunicazione immediata.

21. Incidenti di sicurezza e violazioni dei dati personali

1. Per incidente di sicurezza si intende qualsiasi evento che possa compromettere la riservatezza, l'integrità o la disponibilità dei dati o dei sistemi dell'Istituzione scolastica.
2. A titolo esemplificativo costituiscono incidenti di sicurezza:
   a) perdita o furto di un dispositivo;
   b) invio di dati personali al destinatario errato;
   c) apertura di allegati o collegamenti sospetti;
   d) perdita o divulgazione di credenziali;
   e) accesso non autorizzato a un sistema;
   f) diffusione accidentale di documenti;
   g) malware o sospetta infezione del dispositivo;
   h) cancellazione o alterazione accidentale di dati;
   i) smarrimento di documentazione cartacea;
   l) accesso di terzi a informazioni riservate.
3. In caso di incidente il dipendente deve:
   a) interrompere, ove necessario, l'attività che potrebbe aggravare l'incidente;
   b) non cancellare o alterare volontariamente le eventuali evidenze utili;
   c) informare tempestivamente l'Istituzione scolastica secondo i canali interni;
   d) seguire le istruzioni ricevute;
   e) collaborare alle attività di contenimento e ripristino.
4. Il dipendente non deve autonomamente comunicare all'esterno l'accaduto, salvo quanto previsto dalle procedure dell'Istituzione scolastica.

22. Phishing, malware e altre minacce informatiche

1. Il dipendente deve prestare particolare attenzione ai tentativi di phishing, frode informatica, furto di credenziali e diffusione di malware.
2. In caso di messaggio sospetto il dipendente deve evitare di:
   a) cliccare sui collegamenti;
   b) aprire allegati non attesi;
   c) fornire credenziali;
   d) comunicare dati personali;
   e) installare software richiesti dal messaggio.
3. Eventuali messaggi sospetti devono essere segnalati secondo le procedure di sicurezza informatica dell'Istituzione scolastica.

23. Aggiornamenti e sicurezza del software

1. Il dipendente non deve disattivare gli aggiornamenti di sicurezza dei dispositivi forniti dall'Istituzione scolastica.
2. Gli aggiornamenti devono essere effettuati secondo le indicazioni dell'Amministrazione o dei soggetti incaricati dell'assistenza informatica.
3. È vietata l'installazione di programmi privi di licenza o comunque non autorizzati.
4. Qualora il dispositivo presenti anomalie o comportamenti sospetti, il dipendente deve informare tempestivamente il referente tecnico individuato dall'Istituzione scolastica.

24. Controllo e monitoraggio

1. Gli strumenti informatici e i sistemi messi a disposizione dall'Istituzione scolastica possono essere utilizzati per garantire la sicurezza, la continuità operativa, la protezione dei dati e il corretto funzionamento dei servizi, nel rispetto della normativa vigente.
2. Eventuali sistemi dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori devono essere utilizzati nel rispetto dell'art. 4 della legge 20 maggio 1970, n. 300, delle garanzie previste dalla normativa vigente e delle disposizioni in materia di protezione dei dati personali.

3. Il presente documento non costituisce autorizzazione generale al controllo dell'attività lavorativa mediante strumenti informatici.
4. Le eventuali attività di monitoraggio devono essere proporzionate alle finalità perseguite e rispettare i principi di necessità, proporzionalità, trasparenza e minimizzazione.

Il Garante ha recentemente ribadito che anche strumenti quali log di navigazione e sistemi di conservazione dei dati possono comportare forme di controllo dell'attività dei lavoratori e, ove ricorrano i presupposti, devono essere rispettate le garanzie previste dall'art. 4 dello Statuto dei lavoratori.

25. Diritto alla riservatezza del dipendente

1. Anche nello svolgimento del lavoro agile il dipendente mantiene il diritto alla riservatezza e alla protezione dei propri dati personali.
2. Le informazioni relative all'utilizzo degli strumenti informatici da parte del dipendente possono essere trattate dall'Istituzione scolastica esclusivamente per finalità legittime e nel rispetto della normativa vigente.
3. L'Istituzione scolastica informa il personale, secondo le modalità previste dalla normativa, sui trattamenti di dati personali connessi all'utilizzo degli strumenti informatici e telematici.
4. Il dipendente non è tenuto a consentire forme di controllo ulteriori rispetto a quelle previste dalla legge, dalla contrattazione e dalle disposizioni organizzative legittimamente adottate dall'Istituzione scolastica.

26. Obbligo di collaborazione

1. Il dipendente è tenuto a collaborare con l'Istituzione scolastica per garantire la sicurezza dei dati e dei sistemi informativi.
2. In particolare, il dipendente deve:
   a) seguire le istruzioni ricevute;
   b) partecipare alle attività formative eventualmente organizzate;
   c) segnalare tempestivamente anomalie e incidenti;
   d) rispettare le procedure di sicurezza;
   e) utilizzare correttamente gli strumenti messi a disposizione.

27. Restituzione delle apparecchiature e cessazione dell'accesso

1. Alla cessazione dell'accordo individuale di lavoro agile o del rapporto di lavoro, il dipendente deve restituire le apparecchiature e gli eventuali supporti messi a disposizione dall'Istituzione scolastica secondo le modalità indicate dall'Amministrazione.
2. Il dipendente deve cessare l'utilizzo delle credenziali e degli strumenti di accesso ai sistemi istituzionali quando l'Istituzione scolastica ne disponga la disattivazione.
3. Eventuali copie di documenti o dati dell'Istituzione scolastica presenti su dispositivi personali devono essere eliminate secondo le istruzioni impartite dall'Amministrazione, fermo restando quanto previsto dalle procedure di conservazione documentale.

28. Responsabilità del dipendente

1. Il dipendente è responsabile del rispetto delle presenti istruzioni nell'ambito delle attività a lui assegnate e delle autorizzazioni ricevute.
2. La violazione delle disposizioni in materia di protezione dei dati personali, sicurezza informatica e riservatezza può comportare conseguenze secondo la normativa vigente, il CCNL e il codice disciplinare applicabile.
3. La responsabilità deve essere valutata in relazione alla concreta condotta del dipendente, alle istruzioni ricevute, alle circostanze dell'evento e agli obblighi derivanti dalle mansioni assegnate.

29. Formazione e aggiornamento

1. L'Istituzione scolastica promuove, ove necessario, attività di formazione e aggiornamento rivolte al personale che svolge la prestazione in modalità agile.
2. La formazione può riguardare:
   a) protezione dei dati personali;
   b) sicurezza informatica;
   c) phishing e altre minacce informatiche;
   d) utilizzo sicuro della posta elettronica;
   e) gestione delle credenziali;
   f) utilizzo delle piattaforme istituzionali;
   g) gestione dei documenti digitali;
   h) sicurezza delle postazioni di lavoro;
   i) gestione degli incidenti.
3. Il dipendente è tenuto a partecipare alle attività formative obbligatorie previste dall'Istituzione scolastica.

30. Informazioni e contatti

1. Per questioni relative alla protezione dei dati personali il dipendente può rivolgersi al Responsabile della Protezione dei Dati (RPD/DPO) dell'Istituzione scolastica attraverso i recapiti indicati nell'informativa privacy dell'Istituto.
2. Per questioni relative alla sicurezza informatica, alle apparecchiature e all'accesso ai sistemi il dipendente deve utilizzare i canali di assistenza indicati dall'Istituzione scolastica.

3. Per questioni relative all'organizzazione della prestazione in modalità agile il dipendente si rivolge al Dirigente scolastico o al soggetto da questi individuato.

31. Disposizioni finali

1. Le presenti istruzioni costituiscono parte integrante del Regolamento per la disciplina del lavoro agile del personale ATA.
2. Il dipendente dichiara di aver ricevuto, letto e compreso le presenti istruzioni e si impegna a rispettarle durante tutto il periodo di svolgimento della prestazione in modalità agile.
3. Le presenti istruzioni sono integrate dalle ulteriori disposizioni adottate dall'Istituzione scolastica in materia di:
   a) protezione dei dati personali;
   b) sicurezza informatica;
   c) utilizzo degli strumenti informatici;
   d) posta elettronica;
   e) conservazione documentale;
   f) gestione degli incidenti di sicurezza;
   g) sicurezza sul lavoro.
4. In caso di contrasto tra le presenti istruzioni e disposizioni sopravvenute di legge, regolamento, provvedimento dell'autorità competente o contrattazione collettiva, prevalgono le disposizioni sopravvenute.

DICHIARAZIONE DEL DIPENDENTE

Il/La sottoscritto/a _____

nato/a a _____ il _____

in servizio presso l'Istituzione scolastica _____

con profilo professionale _____

dichiara:

- di aver ricevuto l'**Allegato 4 – Informativa e istruzioni operative per la protezione dei dati personali e la sicurezza informatica nello svolgimento del lavoro agile**;
- di aver preso conoscenza delle disposizioni in esso contenute;
- di impegnarsi a rispettare le istruzioni impartite dall'Istituzione scolastica in materia di protezione dei dati personali, riservatezza e sicurezza informatica;
- di impegnarsi a comunicare tempestivamente eventuali incidenti, smarrimenti, accessi non autorizzati o altre situazioni che possano compromettere la sicurezza dei dati o dei sistemi dell'Istituzione scolastica;
- di essere consapevole che la violazione delle disposizioni applicabili può comportare le conseguenze previste dalla normativa e dalla contrattazione collettiva vigenti.

Luogo e data _____

Firma del dipendente