Prot. 124 1/2P Brescia, 22.06.2023

REGOLAMENTO INFORMATICO

DELL'ISTITUTO

LICEO INTERNAZIONALE PER L'IMPRESA GUIDO CARLI

1.1. Ambito di Applicazione

1. Il presente regolamento si applica a tutti i trattamenti dei dati personali gestiti dall'organizzazione e a tutti coloro che a titolo di disegnati/autorizzaTi al trattamento si trovino ad operare con dati di Fondazione A.I.B – Divisione Liceo Internazionale per l'Impresa Guido Carli Via Stretta, 175 – 25136 Brescia, 030 221086, e-mail privacy@liceoguidocarli.eu PEC fondazioneaib@legalmail.it.

1.2. Principi generali

1. Il trattamento dei dati personali dovrà avvenire rispettando i principi di riservatezza, correttezza, liceità e trasparenza come previsto dal GDPR.
2. Il trattamento dei dati personali dovrà avvenire esclusivamente per le finalità indicate dal Titolare del Trattamento. Ogni autorizzato dovrà trattare esclusivamente i dati per il quale è stato autorizzato e per lo svolgimento delle mansioni affidate.
3. L'Istituto è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.
4. L'organizzazione è esclusiva titolare e proprietaria dei dispositivi messi a disposizione degli autorizzati, ai soli fini dell'attività lavorativa.
5. Qualora l'organizzazione dovesse assegnare dispositivi al designato, autorizzato si ricorda che l'uso è esclusivamente per fini di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare. Qualsiasi eventuale tolleranza da parte di questo istituto, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente regolamento
6. L'utilizzo della posta elettronica d'istituto è connesso allo svolgimento dell'attività lavorativa.

2. SEZIONE: OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

Il responsabile/autorizzato deve mettere in sicurezza il dispositivo utilizzato per il trattamento dei in caso di allontanamento dalla postazione lavorativa affinché persone non autorizzate non abbiano accesso ai dati protetti. In particolare, dovrà essere attivata la funzione di blocco della postazione o del dispositivo.

Gli autorizzati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti. In caso di allontanamento, eventuali documenti cartacei contenenti dati personali, devono essere riposti negli appositi armadi di sicurezza.

Non devono essere lasciati incustoditi documenti cartacei contenenti dati personali.

La stampa di documenti contenenti dati personali non deve essere inviata a stampanti in utilizzo condiviso dove possa essere vista o prelevata da personale non autorizzato.

3 SEZIONE: STRUMENTI DI LAVORO

3.1 COMPUTER ISTITUTO

L'accesso ai dispositivi è protetto da password che deve essere custodita dall' autorizzato con la massima diligenza e non divulgata. Per necessità d'istituto gli amministratori di sistema utilizzando il proprio login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server d'istituto nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare, il designato/autorizzato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete d'istituto per creare, registrare e file legati all'attività lavorativa

2. Non modificare le configurazioni già impostate sul personal computer.

3. Non Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta d'istituto

4. Non creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses e malware in genere.

5. Non accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

6. Non effettuare in proprio attività manutentive o permettere questo tipo di attività a terzi non autorizzati.

7. Non installare alcun software di cui l'istituto non possieda la licenza.

8. Non aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, , ecc.), senza l'autorizzazione espressa dell'organizzazione; per scaricare file o documenti contenenti dati personali o particolari raccolti dal Titolare destinati ad utilizzo esterno dell'istituto.

9. È vietato ostacolare l'azione dell'antivirus istituto.

10. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute.

L'autorizzato che sospetta un malfunzionamento dello strumento informatico dovrà tempestivamente o entro 2 ore da quando ne viene a conoscenza informare l'amministratore di sistema di sede, che provvederà a risolvere il problema.

Nel caso di esclusione o malfunzionamento o un'ipotetica compromissione dello strumento informatico, questa dovrà essere isolata dal sistema dall'amministratore di rete.

3.2 L'utilizzo del notebook, tablet o smartphone istituto

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa d'istituto al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili. Sui dispositivi mobili d'istituto è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'istituto.

L'autorizzato è responsabile del dispositivo affidatogli, l'eventuale furto o smarrimento del dispositivo deve essere immediatamente segnalato anche all'istituto, per eventuali provvedimenti di sicurezza.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

3.3. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli autorizzati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

3.4. Dispositivi personali (BYOD).

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali se non autorizzati.

3.5. Utilizzo del cellulare/smartphone personale.

E' consentito un utilizzo moderato dei dispositivi personali durante l'orario di lavoro.

Agli autorizzati ai quali è stata assegnata sim d'istituto è consentito l'uso di dispositivi personali, previa valutazione dell'istituto rispetto alle misure di protezione dei dati, in mancanza di dispositivi d'istituto.

I consulenti e collaboratori esterni, possono utilizzare i propri cellulari/smartphone per memorizzare dati d'istituto solo se espressamente autorizzati dall'istituto stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dall'istituto, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

3.6. Restituzione dei dispositivi e distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli autorizzati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'istituto, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare, l'istituto provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'autorizzato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'istituto, della permanenza dei presupposti per l'utilizzo dei dispositivi d'istituto e dei dati dell'istituto i responsabili/autorizzati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dispositivi in uso previa cancellazione di qualsiasi dato personale
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati d'istituto in essi contenuti, tramite qualsiasi processo.

4 SEZIONE PASSWORD

L'autorizzato per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri.
2. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi.
3. La parola chiave dovrà essere modificata nel caso in cui venga comunicata a terze persone.
4. Le credenziali, laddove utilizzate, non possono essere assegnate ad altri utenti, neppure in tempi diversi.
5. Le credenziali non utilizzate da almeno tre mesi sono disabilitate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
6. Occorre cambiare immediatamente una password, non appena si abbia alcun dubbio che sia diventata poco "sicura".
7. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri.

8. La password non deve contenere informazioni riconducibili direttamente o indirettamente al responsabile/autorizzato come nome e cognome propri o di parenti, numero matricola, data di nascita).
9. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare). Potranno invece essere memorizzate su dispositivi di password Manager.
10. Evitare di digitare la propria password in presenza di altri soggetti, anche se collaboratori o dipendenti dell'istituto.

4.1 Blocco e disattivazione delle credenziali.

Dopo 10 tentativi falliti di accesso, l'account viene bloccato e si può richiedere lo sblocco e il ripristino della password di default da cambiare all'amministratore del sistema.

Le credenziali che non vengono utilizzate da parte dei responsabili/autorizzati per un periodo superiore ai sei mesi verranno disattivate dall'istituto. In qualsiasi momento, l'organizzazione si riserva il diritto di revocare al responsabile/autorizzato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

5 SEZIONE: INTERNET

5.1. Misure preventive per ridurre navigazioni illecite

L'utilizzo di internet da parte del designato/autorizzato deve avvenire esclusivamente per finalità attinenti alle mansioni assegnate dal Titolare del Trattamento

Pertanto, il responsabile/autorizzato non deve:

- partecipazione a forum non professionali, bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione;
- memorizzare di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'istituto stesso. L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.
- creare siti web e/o applicazioni personali con gli strumenti e sui sistemi dell'organizzazione;
- accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'istituto per bloccare accessi;
- il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall'organizzazione.
  Ogni utilizzo illegittimo di Internet, nonché un possibile illecito trattamento di dati personali e particolari, è posta sotto la personale responsabilità del Responsabile/autorizzato inadempiente.

6 SEZIONE VI

POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro

I Responsabili/incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

L'interessato non può rivalersi sull'ente in caso in cui una violazione dei dati coinvolga dati di natura personale non legati all'attività lavorativa.

All'atto di assunzione verrà assegnato al dipendente un account di posta elettronica. L'indirizzo d'istituto è fornito esclusivamente per svolgere attività lavorativa

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'utilizzo della mail d'istituto è consentito esclusivamente per finalità istituzionali.

In ogni caso,

1. In caso di ricezione sulla e-mail d'istituto di posta personale, si avverte di cancellare immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile back up dei dati.

2. Avvisare l'Amministratore di rete quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

3. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa utilizzando le credenziali (la casella di posta elettronica e password) già utilizzate per servizi di ente.

4. Utilizzare il disclaimer indicato dal Titolare del Trattamento

5. È vietato creare, archiviare o spedire, anche solo all'interno della rete d'istituto, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, propaganda elettorale, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo istituzionale.

6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti d'istituto, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni; qualora si rendesse necessario il trasferimento di file utilizzare gli opportuni sistemi di memorizzazione in cloud messi a disposizione dall'organizzazione.

6.3 Accesso ai servizi di posta elettronica e gestione della stessa

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica d'istituto per motivi diversi da quelli strettamente legati all'attività lavorativa.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

l'invio e/o la ricezione di allegati non legati all'attività lavorativa;

l'invio e/o la ricezione di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list (salvo sia necessario per finalità lavorative);

la partecipazione a catene telematiche (o di Sant'Antonio).

Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Esaurito lo spazio assegnato, l'utente potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione o lo "scarico" dei messaggi di posta.

Ogni comunicazione, inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'istituto ovvero contenga documenti da considerarsi riservati, in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere comunicata al responsabile dell'area e tutti gli atti rilevanti o con impegni preconrattuali -contrattuali dovranno essere salvati sul server dell'istituto.

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

Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (per esempio pec, raccomandata a/r), devono essere autorizzate e firmate dal legale rappresentante o suo delegato.

È obbligatorio porre la massima attenzione nell'aprire i file "allegati" di posta elettronica prima del loro utilizzo.

Al fine di garantire la funzionalità del servizio di posta elettronica d'istituto e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, l'utente, in caso di assenze programmate (per esempio ferie o attività di lavoro fuori sede dell'assegnatario della casella), provvederà ad attivare la funzionalità di invio automatica di messaggi di risposta contenenti i riferimenti di un altro soggetto o altre utili modalità di contatto della struttura.

6.4 utilizzo della posta elettronica in caso di assenza

Nel caso in cui il lavoratore sia assente (ad esempio per ferie, permessi o attività di lavoro fuori sede ecc..) dovrà impostare la propria casella e-mail istituzionale in maniera tale da consentire l'invio automatico di messaggi di risposta contenenti le coordinate (anche elettroniche o telefoniche) di un altro soggetto o di altre utili modalità di contatto d'istituto.

In caso di assenza non programmata (per esempio malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura d'istituto tramite l'amministratore di sistema.

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il dipendente deve delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al datore di lavoro quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Qualora il dipendente non riesca a delegare altro lavoratore, il datore di lavoro previo reset delle password potrà verificare il contenuto di messaggi e inoltrarsi quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Al termine delle operazioni redigerà apposito verbale e informerà il lavoratore alla prima occasione utile.

Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando che il personale debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy di istituto.

Una copia di tutti i messaggi di posta elettronica presenti sul server è salvata con procedure di "backup" a cadenza giornaliera.

Qualora l'utente "scarichi" sulla propria postazione di lavoro ovvero cancelli i messaggi di posta ancora presenti sul server, tali messaggi non saranno oggetto di "backup".

Fare attenzione al phishing, tentativo di truffa realizzato solitamente sfruttando la posta elettronica o applicazioni di messaggistica istantanea, che ha per scopo il furto di informazioni e dati personali. I mittenti delle e-mail di phishing sembrano essere organizzazioni conosciute, come banche o servizi web, e hanno apparentemente uno scopo informativo: avvisano di problemi riscontrati con account personali dell'utente (per esempio home banking, portali, provider di posta elettronica, social network, etc...) e forniscono suggerimenti su come risolvere le problematiche.

Nella maggioranza dei casi vengono simulate situazioni molto comuni come la scadenza di una password, il cambiamento di condizioni contrattuali, il rinnovo della carta prepagata e anche problemi inerenti ad accrediti, addebiti e trasferimenti di denaro online.

Il tutto si presenta in maniera molto verosimile grazie alla presenza di un collegamento a un sito web che ha le fattezze di quello originale.

Nel caso in cui si cliccasse sul collegamento e si fornissero le informazioni richieste, l'utente darà il completo accesso del suo account alla persona o all'organizzazione che ha effettuato l'attacco.

In caso di dubbio è buona norma sentire chi "dovrebbe" aver inviato il messaggio ed appurare che sia effettivamente legittimo, oppure chiedere supporto al tecnico informatico.

6.5 disattivazione account

In caso di cessazione del rapporto di lavoro verrà disattivato l'account di posta elettronica dell'istituto con le seguenti modalità conformi al provvedimento del Garante Privacy del 04.12.2019:

Dalla data di cessazione del rapporto di lavoro e fino a 45 giorni successivi a tale data la casella non verrà di disattivata e verrà attivato dal tecnico IT un sistema di risposta automatica al fine di rendere noto all'esterno il nuovo riferimento interno istituzionale. Il messaggio tipo potrebbe essere il seguente: "Il presente indirizzo di posta elettronica non è più attivo, poiché titolare della casella di posta elettronica istituzionale _____, ha cessato il proprio rapporto di collaborazione con la nostra Società. A far data da _____ [45 giorni dopo la cessazione] tale indirizzo di posta elettronica verrà definitivamente disattivato. Fino alla data sopraindicata ogni eventuale e-mail inviata al citato indirizzo di posta elettronica sarà inoltrata al seguente indirizzo: _____. Vi preghiamo di prendere nota di quanto sopra e di cortesemente aggiornare le Vostre rubriche. Cordiali saluti".

Durante tale fase l'account non sarà accessibile e sarà assolutamente vietato rispondere o scrivere e-mail con l'account del lavoratore cessato.
- Decorsi 45 giorni dalla data di cessazione del rapporto lavorativo l'account verrà definitivamente disattivato.

7 SEZIONE: SISTEMI IN CLOUD

È vietato ai responsabili/incaricati l'utilizzo di sistemi cloud non espressamente approvati dall'istituto.

8 SEZIONE: GESTIONE DATI CARTACEI

I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento e non devono comunque rimanere incustoditi su scrivanie tavoli di lavori

In caso di errore nell'esecuzione di una fotocopia di un documento che contiene dati personali questa potrà essere cestinata solo dopo essere stata distrutta

A seguito di una cessazione del rapporto di lavoro o di consulenza tutti i dati cartacei dovranno essere restituiti al Titolare del trattamento. i documenti non dovranno essere alterati o manomessi in nessun modo.

9 SEZIONE: APPLICAZIONE E CONTROLLO

9.1 Il controllo

L'istituto, in qualità di Titolare degli strumenti informatici, dei dati si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

− Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.

− Evitare la commissione di illeciti o per esigenze di carattere difensivo.

− Verificare la funzionalità del sistema e degli strumenti informatici. Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

9.2. Modalità di verifica

L'istituto informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli autorizzati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

In caso di anomalie, l'istituto, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia. In tali casi, il controllo si concluderà con un avviso al Responsabile dell'Area interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti istituzionali affinché lo stesso inviti gli autorizzati di quell'area ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'istituto si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi d'istituto

9.3. Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

− Ad esigenze tecniche o di sicurezza del tutto particolari.

− All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria.

− All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

10 SEZIONE: SMARTWORKING

ll lavoro in modalità smartworking è una modalità di svolgimento dell'attività lavorativa saltuariamente effettuata al di fuori dei locali dell'istituto e con l'uso di tecnologie informatiche in remoto.

Tali tecnologie sono di proprietà dell'organizzazione e devono essere utilizzate secondo le linee guida indicate in precedenza.

Nel caso in cui i dipendenti utilizzino strumenti personali l'organizzazione deve analizzare le tipologie di trattamenti effettuati e in base a questi definire le misure di sicurezza da applicare come per esempio VPN.

Il datore di lavoro rimarrà dunque responsabile dell'adozione di misure volte a salvaguardare i dati utilizzati ed elaborati dai propri dipendenti, ma questi ultimi saranno chiamati ad un comportamento particolarmente diligente, tanto in tema di custodia degli strumenti tecnologici, quanto di conservazione e riservatezza dei dati.

11 SEZIONE: PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto del presente Regolamento potrà comportare una sanzione in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato.

10.1. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere, ai sensi dell'art. 15 del Regolamento Europeo 2016/679, alle informazioni che lo riguardano scrivendo al Titolare del Trattamento o al Responsabile della Protezione dei Dati secondo le modalità definite nella Procedura di Gestione dei Diritti degli Interessati.

11 SEZIONE: VALIDITA', AGGIORNAMENTO

11.1. Validità

Il presente regolamento ha validità a partire da 22.06.2023

11.2. Aggiornamento

Il presente regolamento sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative. Ogni variazione del presente sarà comunicata prontamente agli autorizzati al trattamento.

Il Titolare del Trattamento

Fondazione A.I.B – Divisione Liceo Internazionale per l'Impresa Guido Carli