COGNITA

Europa

Policy IT regionale

Versione per l'Italia

Settembre 2024

41-42 Eastcastle Street, Londra W1W 8DY, Regno Unito. T +44 (0)20 7636 8444. w w w . c o g n i t a . c o m
Cognita Schools Limited No 02313425. Sede legale: Seebeck House, One Seebeck Place, Knowlhill, Milton Keynes MK5 8FR

Contenuti

1 Introduzione

L'uso della tecnologia come strumento e abilitatore è diventato parte integrante della vita scolastica e domestica. Cognita è impegnata nell'uso efficace e mirato della tecnologia per l'insegnamento, l'apprendimento e l'amministrazione ed è pienamente impegnata a proteggere il suo personale (compresi gli appaltatori e gli insegnanti peripatetici), gli studenti, i genitori e i visitatori, collettivamente "stakeholder", dall'uso illegale o dannoso della tecnologia da parte di individui o gruppi, sia consapevolmente che inconsapevolmente.

Cognita promuove attivamente la partecipazione dei genitori per aiutare la scuola a salvaguardare il benessere degli studenti e a promuovere un uso sicuro della tecnologia.

Questa policy si applica all'uso delle apparecchiature, delle applicazioni e dei servizi informatici, collettivamente "tecnologia" (sia in sede che fuori sede), forniti e/o messi a disposizione degli interessati attraverso le reti della scuola e/o degli uffici regionali.

Una copia di questa policy è disponibile su richiesta e pubblicata sul sito web della scuola.

In caso di violazione di questa policy, la mancata lettura di questa policy non sarà accettata come difesa da nessuna delle parti interessate. In tali casi, Cognita si riserva il diritto di indagare e di intraprendere le azioni necessarie.

2 Scopo della policy

2.1 Promuovere una cultura del comportamento responsabile, dell'uso sicuro e della cura di qualsiasi tecnologia a disposizione degli stakeholder sia nelle scuole che negli uffici regionali (sia in sede che fuori sede).

2.2 Delineare l'uso accettabile e inaccettabile della tecnologia nelle scuole e negli uffici regionali (sia in sede che fuori sede).

2.3 Delineare i principali ruoli e responsabilità di tutti gli stakeholder quando si utilizza la tecnologia Cognita.

2.4 Educare e incoraggiare gli studenti a fare buon uso delle opportunità educative offerte dall'accesso alla tecnologia nella loro scuola.

2.5 Salvaguardare e promuovere il benessere degli studenti, in particolare anticipando e prevenendo i rischi derivanti da:

- Esposizione deliberata o involontaria a contenuti dannosi e/o inappropriati come contenuti pornografici, razzisti, estremisti e/o altri contenuti offensivi.
- Contatti inappropriati da parte di adulti conosciuti al di fuori della scuola e/o da parte di estranei
- Comportamento inappropriato nell'uso della tecnologia
- Cyber-bullismo e/o abuso online
- Copia e condivisione dei dati personali
- Preoccupazioni e rischi di natura commerciale, ad esempio frodi, truffe e/o estorsioni.

2.6 Delineare il processo e i requisiti per la segnalazione dell'uso improprio della tecnologia e degli incidenti.

2.7 Garantire a tutti i soggetti interessati la sicurezza e l'incolumità.

3 Ambito di applicazione della policy

3.1 Questa policy si applica a tutte le scuole e agli uffici Cognita interessati.

3.2 Le scuole adotteranno un approccio ampio e mirato nel considerare ciò che rientra nel significato di tecnologia. Questa policy si riferisce a tutti i dispositivi tecnologici, informatici e di comunicazione, all'hardware di rete, al software e ai servizi ad essi associati, compresi, ma non solo, i seguenti:

- La rete scolastica, il WIFI e l'accesso a Internet
- Dispositivi hardware e digitali, compresi i dispositivi "intelligenti".
- Software (basato su cloud e on-premise)
- Applicazioni di comunicazione e collaborazione (ad es. e-mail, Microsoft Teams, WhatsApp, Snapchat)
- Ambienti di apprendimento virtuale
- Social media (ad es. Facebook, Instagram, Tik Tok, X - ex Twitter)

Questa policy si applica a qualsiasi membro della comunità scolastica in cui la cultura o la reputazione della scuola e/o delle parti interessate siano messe a rischio dai suoi comportamenti o dalle sue azioni.

4 Ruoli e responsabilità

Questo documento di policy è di responsabilità del Responsabile IT di Cognita Europe & North America, che deve assicurare che la tecnologia sia distribuita e monitorata in linea con questa policy e con le altre politiche pertinenti.

4.1. I Direttori Generali POD (Regno Unito), il Direttore Generale (Spagna, Italia e Svizzera) e i Direttori scolastici sono responsabili della pubblicazione di questa policy e della sua continua attuazione e monitoraggio a livello scolastico.

4.2. Tutte le parti interessate sono responsabili dell'osservanza della policy.

4.3. Il responsabile della sicurezza informatica è responsabile dei servizi informatici e del processo di filtraggio e monitoraggio.

4.4. Il Designated Safeguarding Lead (DSL) è responsabile (con il supporto delegato di supplenti e/o colleghi informatici) di avere una visione d'insieme della salvaguardia e della sicurezza online. Questo include (ma non si limita a):

- Monitorare l'attività online degli studenti e compilare i relativi registri (ulteriori dettagli nell'Appendice A - Dichiarazione sul filtraggio del web).
- Seguire i problemi di salvaguardia relativi alla comunicazione digitale o tutte le questioni relative all'IT riguardanti gli studenti, i loro genitori o accompagnatori e le agenzie esterne, come richiesto (ulteriori dettagli nella Policy di Salvaguardia di Cognita).
- sollevare qualsiasi preoccupazione complessa in relazione al monitoraggio dei dispositivi e/o ai risultati di questo in relazione ai singoli studenti con il responsabile regionale della salvaguardia (che si rivolgerà, se necessario, al responsabile europeo dell'IT se la questione coinvolge una componente tecnologica)
- Garantire che il personale sia formato in termini di sicurezza online per i bambini e come riconoscere i rischi e gli indicatori di preoccupazione.
- Garantire che i bambini vengano istruiti su come tenersi al sicuro online e sui potenziali rischi dell'attività online.

5 Uso sicuro della tecnologia

5.1. La scuola si impegna a utilizzare in modo sicuro e mirato la tecnologia per l'insegnamento, l'apprendimento e l'amministrazione.

5.2. L'uso della tecnologia deve essere sicuro, responsabile, rispettoso degli altri e legale. Gli stakeholder sono responsabili delle loro azioni, della loro condotta e del loro comportamento quando utilizzano la tecnologia in ogni momento.

5.3. La scuola sosterrà l'uso della tecnologia e renderà l'accesso a Internet il più possibile illimitato, bilanciando al contempo le esigenze educative, la sicurezza e il benessere delle parti interessate, nonché la sicurezza e l'integrità dei nostri sistemi.

5.4. Sono disponibili strumenti di monitoraggio, registrazione e allerta per mantenere la sicurezza, la salvaguardia e la protezione della tecnologia a tutela degli stakeholder.

5.5. Gli strumenti di filtraggio e monitoraggio vengono rivisti a livello centrale su base annuale per garantire che l'attuale dotazione risponda a tutte le esigenze del personale e degli studenti. Questa revisione coinvolge i colleghi dei settori IT, Cyber Security e Safeguarding, nonché i governatori e i proprietari.

5.6. Nell'interesse della tutela degli studenti, i dispositivi 1-to-1 degli studenti sono dotati di un software di monitoraggio preinstallato che blocca alcuni siti e fornisce dati storici e in tempo reale sull'utilizzo del dispositivo, ad esempio la navigazione web. I dati raccolti vengono conservati per un periodo massimo di 90 giorni.

5.7. Il software di monitoraggio utilizza l'intelligenza artificiale (AI) per determinare come vengono filtrati i nuovi siti web e quali categorie rientrano nei loro contenuti (ulteriori dettagli nell'Appendice A).

5.8. Il Supporto IT e la Direzione IT hanno l'autorità di apportare modifiche manuali al sistema di filtraggio nelle scuole, a condizione che abbiano l'approvazione del Senior Leadership Team (SLT) della scuola e/o dell'IT regionale.

5.9. Il team di tutela della scuola è responsabile della supervisione dei sistemi e dei processi di monitoraggio in vigore. I team di tutela della scuola controllano regolarmente l'uso dei dispositivi scolastici da parte degli studenti, dando priorità agli studenti vulnerabili, ma effettuando anche controlli casuali laddove possibile. È disponibile una formazione per aiutare il personale a comprendere come analizzare i dati di filtraggio all'interno del sistema Lightspeed.

5.10. Tutto il personale, e coloro che hanno la supervisione della governance, hanno una formazione annuale di sensibilizzazione sulla cybersecurity.

Tutto il personale deve comprendere le aspettative e le responsabilità relative al sistema di filtraggio. Tutto il personale deve comprendere che il sistema di filtraggio è in atto per salvaguardare gli studenti da contenuti online dannosi, compresi quelli relativi a (ma non solo) pornografia e contenuti maturi/adulti, radicalizzazione, violenza, odio e razzismo, attività criminali e terrorismo*. L'adeguatezza di qualsiasi sistema di filtraggio e monitoraggio è di competenza delle singole scuole in base agli standard Cognita. La scuola può richiedere che vengano apportate modifiche su misura al sistema di filtraggio per la propria scuola, da richiedere tramite il Service Desk Cognita o il Responsabile IT.

5.11. Vogliamo che gli studenti si divertano a usare la tecnologia e che diventino utenti esperti, poiché la tecnologia è diventata una parte fondamentale dell'istruzione, non solo come veicolo per offrire un insegnamento e un apprendimento eccellenti, ma anche come piattaforma per la collaborazione e la produttività.

5.12. È responsabilità di ogni scuola educare gli studenti all'importanza di un uso sicuro e responsabile della tecnologia per proteggere se stessi e gli altri online. L'IT regionale supporta questo aspetto attraverso varie risorse e politiche (tra cui questa).

5.13. Cognita incoraggia il feedback e la partecipazione dei genitori, ad esempio attraverso il sondaggio "Voice of the Parent" (VoP), per contribuire a promuovere l'uso sicuro della tecnologia per gli studenti.

5.14. Qualsiasi preoccupazione relativa a un uso non sicuro o inappropriato della tecnologia deve essere segnalata a un membro dell'SLT, al Direttore della scuola o al Designated Safeguardin Leader (DSL) o al Service Desk di Cognita lo stesso giorno in cui viene individuata la preoccupazione.

5.15. Qualsiasi incidente grave che coinvolga un uso non sicuro o inappropriato della tecnologia deve essere segnalato immediatamente dal Direttore della scuola e/o dal DSL al Cognita Europe Head of IT and United States (per le questioni tecnologiche) e al Regional Safeguarding Lead (per le questioni di salvaguardia), che lavoreranno con i colleghi competenti per registrare, indagare e mitigare i rischi relativi all'incidente. La scuola deve compilare un Modulo di Segnalazione di Incidente Grave (SIRF), a seguito delle indagini e degli interventi effettuati con il supporto della Direzione Regionale IT e Salvaguardia.

5.16. Tutti gli utenti della tecnologia possono trovare utili le seguenti risorse per mantenere se stessi e gli altri al sicuro online:

- Centro Safer Internet del Regno Unito
- Questioni di Internet - risorse
- Sicurezza della famiglia Google
- Common Sense Media

Commentato [JB1]: Aggiungete i riferimenti italiani se lo desiderate

Inoltre, le scuole dovrebbero prendere in considerazione la possibilità di soddisfare gli standard di sicurezza informatica stabiliti dal governo e/o dalle autorità locali.

Per sostenere le scuole nell'adempimento di questo dovere, sono stati pubblicatistandard di filtraggio e monitoraggio che stabiliscono che le scuole devono

- Identificare e assegnare ruoli e responsabilità per la gestione dei sistemi di filtraggio e monitoraggio.
- Rivedere le disposizioni in materia di filtraggio e monitoraggio almeno una volta all'anno.
- Bloccare i contenuti dannosi e/o inappropriati (ad esempio immagini esplicite, contenuti violenti o di odio e altre forme di media dannosi) senza impattare in modo irragionevole sull'insegnamento e l'apprendimento.
- disporre di strategie di monitoraggio efficaci che rispondano alle loro esigenze di salvaguardia.

6 Diritto all'uso della rete e delle attrezzature della scuola e dell'ufficio

6.1. I dipendenti e gli studenti della scuola riceveranno un nome utente e una password per accedere ai dispositivi e ai servizi tecnologici. **Non** devono permettere ad altri di utilizzare il loro account e non devono condividere le password con nessuno.

6.2. Gli account di posta elettronica della scuola devono essere accessibili solo attraverso Microsoft Office 365 o Google e tutti gli altri servizi di posta elettronica di terze parti **non sono** consentiti.

6.3. Alcune risorse condivise (disponibili a scuola e negli uffici per l'uso da parte di dipendenti e studenti) avranno un nome utente e una password generici per l'accesso e saranno gestite dal docente.

6.4. Tutta la tecnologia scolastica rimane di proprietà di Cognita. La scuola può ragionevolmente richiedere il dispositivo o ritirare l'accesso al servizio, per qualsiasi studente, in qualsiasi momento e, se applicabile, il dispositivo deve essere restituito alla scuola dallo studente.

6.5. Solo i dispositivi scolastici devono essere collegati alla rete della scuola e i dispositivi personali devono collegarsi alla rete degli ospiti, se consentito da un membro dell'SLT della scuola.

6.6. I dispositivi personali del personale non devono essere utilizzati per attività lavorative all'interno della scuola e non devono mai essere utilizzati in presenza di studenti.

6.7. È vietato qualsiasi tentativo di accesso o utilizzo di account, indirizzi e-mail o risorse informatiche appartenenti a un altro stakeholder, a meno che il tentativo non sia effettuato dall'IT regionale per motivi aziendali legittimi e/o sia stato autorizzato tramite un modulo di richiesta di accesso alla casella di posta e ai file.

6.8. I dispositivi designati possono essere forniti ai dipendenti e agli studenti della scuola per l'insegnamento, l'apprendimento e l'amministrazione:

- Agli studenti a cui è stato assegnato un dispositivo 1-to-1 può essere richiesto di firmare il Contratto di utilizzo dell'iPad/Laptop (link in appendice).
- Gli studenti che dispongono di un dispositivo 1-to-1 possono utilizzarlo durante le lezioni su indicazione dell'insegnante.
- I dipendenti della scuola e gli studenti sono responsabili della sicurezza del dispositivo loro assegnato quando lo portano fuori dalla scuola.
- I dispositivi rilasciati dalla scuola e le periferiche associate devono essere restituiti in buone condizioni (escludendo l'usura ordinaria) e funzionanti al termine del periodo di studio o di lavoro presso la scuola.
- I dispositivi del personale danneggiati e/o difettosi vengono riparati o sostituiti e i costi sono coperti a livello centrale o dalla scuola.
- I genitori sono responsabili del costo di una "riparazione" o di una sostituzione "uguale" di un dispositivo assegnato (secondo le indicazioni della scuola) in caso di danneggiamento, volontario, per negligenza o accidentale. Il massimale è di 500€ per ogni danno. Se un dispositivo è irrimediabilmente danneggiato o perso/rubato, i genitori sono responsabili dell'intero costo di sostituzione. Ogni caso sarà valutato individualmente. La responsabilità e i costi associati possono essere contestati, ma la decisione della scuola è definitiva e non può essere impugnata".

7 Uso appropriato della tecnologia per la sicurezza digitale

7.1. La scuola mette a disposizione degli interessati **account di sistema e di applicazione** per scopi didattici e amministrativi.

7.2. Le parti interessate **non devono**:

- Consentire a chiunque di utilizzare il proprio account, a meno che non sia autorizzato (per iscritto) dall'SLT e/o dal Team IT regionale.
- Utilizzare l'account di qualcun altro
- Lasciare il proprio dispositivo sbloccato e/o collegato al proprio account quando non lo si utilizza.
- Utilizzare applicazioni di messaggistica mobile per comunicare con i genitori e/o il personale con gli studenti.
- Inviare messaggi e/o e-mail da account scolastici che sembrano provenire da una persona diversa da quella che ha effettivamente inviato il messaggio, a meno che non sia stato approvato da un membro dell'SLT della scuola.
- Inviare messaggi e/o e-mail relativi al lavoro a/da un account personale.

7.3. La scuola fornisce **hardware e software** a supporto dell'istruzione e del funzionamento della scuola.

- Gli utenti delle apparecchiature tecnologiche della scuola sono tenuti a prendersene cura attraverso un comportamento responsabile.
- La tecnologia scolastica **non deve** essere rimossa dal sito della scuola, tranne nei casi in cui:
    - Il dispositivo è assegnato a un singolo membro del personale; oppure
    - Il dispositivo viene assegnato a uno studente tramite il programma 1-to-1; oppure
    - Esiste un'autorizzazione scritta da parte di un membro dell'SLT.

- La tecnologia scolastica assegnata al personale e agli studenti è responsabilità dell'assegnatario.
- Gli interessati **non devono** lasciare incustodite le apparecchiature tecnologiche portatili, compresi i dispositivi in dotazione alla scuola, a meno che tali apparecchiature non siano fuori uso (a causa di un guasto o semplicemente per aver effettuato la disconnessione e lo spegnimento), nel qual caso devono essere conservate in modo sicuro.
- Lo smarrimento o il danneggiamento della tecnologia scolastica deve essere segnalato a un insegnante, a un membro dell'SLT o al team di assistenza informatica il giorno stesso.
- Il furto di tecnologia scolastica assegnata a un singolo membro del personale o a uno studente tramite il programma 1-to-1 deve essere denunciato alla Polizia e comunicato a un insegnante, a un membro dell'SLT o al team di supporto informatico lo stesso giorno con il numero di riferimento del crimine della Polizia. Se il furto è avvenuto all'interno della scuola, un membro dell'SLT farà la denuncia alla Polizia.
- L'abuso o il danneggiamento deliberato delle apparecchiature tecnologiche della scuola comporterà la fatturazione dell'intero costo di sostituzione o riparazione dell'apparecchiatura alla persona o alle persone responsabili.

Le parti interessate **non devono**:

- Tentare di installare software o applicazioni non approvate sui dispositivi scolastici.
- Scaricare o accedere a software illegale sui dispositivi scolastici.
- Scaricare qualsiasi pacchetto software dalla rete scolastica su supporti portatili o dispositivi personali, a meno che non abbiano l'autorizzazione scritta di un membro dell'SLT e del responsabile di It Europe.
- Tentare di copiare o rimuovere software da un dispositivo scolastico.
- Tentare di alterare la configurazione dell'apparecchiatura hardware o di qualsiasi software di accompagnamento, se non dietro istruzione scritta dell'SLT e/o dell'IT regionale.

7.4. La scuola mette a disposizione risorse tecnologiche per l'accesso e l'archiviazione dei dati e dispone di sistemi di filtraggio per bloccare l'accesso a materiale non idoneo, laddove possibile, per proteggere il benessere degli interessati (ulteriori dettagli nell'Appendice A - Dichiarazione sul filtraggio del web).

I soggetti interessati **non devono**:

- Aggirare i sistemi di filtraggio dei siti web e/o i sistemi di sicurezza tecnologica (tramite navigazione "Tor", estensioni del browser e/o VPN o sistemi simili) mentre si utilizzano i dispositivi della scuola in sede e/o fuori sede.
- accedere o tentare di accedere a dati per i quali non sono autorizzati
- Interferire con il lavoro digitale di altri utenti
- Condividere informazioni private, sensibili e/o confidenziali a meno che:
    - hanno l'autorità di condividere
    - il metodo di condivisione è sicuro e non utilizza identificatori
    - il destinatario è autorizzato a ricevere tali informazioni
    - ci sono motivi di salvaguardia (in questo caso solo il team di salvaguardia può condividere)

È responsabilità degli utenti della tecnologia, quando accedono ai dati, essere consapevoli della violazione dei diritti di proprietà intellettuale, compresi i diritti d'autore, i marchi, i brevetti, il design e i diritti morali.

7.5. La scuola si impegna a salvaguardare e, ove possibile, a mitigare tutti i rischi **di sicurezza** associati alla tecnologia e, se necessario, si impegna a collaborare con l'IT regionale.

7.6. Le preoccupazioni relative a uno dei seguenti aspetti devono essere segnalate al responsabile o a un membro dell'SLT che, a seconda delle necessità, contatterà il responsabile regionale per la salvaguardia e/o il team IT regionale il più presto possibile nello stesso giorno:

- Accesso a materiale/contenuti non idonei su un dispositivo scolastico o sulla rete scolastica.
- Uso improprio della tecnologia che ha causato danni o abusi a un'altra persona (o che è probabile/potenziale che lo faccia) - in modo proporzionato, caso per caso.
- Preoccupazioni relative a virus e altri software dannosi
- e-mail, link e/o siti web sospetti o qualsiasi altra comunicazione

7.7. È responsabilità di tutti gli utenti della tecnologia garantire il **benessere** proprio e degli altri sia sui dispositivi personali che su quelli scolastici. I soggetti interessati **non devono**:

- Usare la propria tecnologia o quella della scuola per fare atti di bullismo online (cyberbullismo) o disturbare l'apprendimento degli altri.
- Usare la propria tecnologia o quella della scuola per entrare in contatto o interagire con persone che non conoscono.
- Utilizzare la propria tecnologia o quella della scuola per creare, archiviare o condividere contenuti sessuali e/o inappropriati/illegali, compresi immagini, audio, video e/o testi.

Le parti interessate devono:

- Segnalare tempestivamente a un insegnante, a un membro del team dirigenziale della scuola o al DSL/CPC qualsiasi preoccupazione relativa al benessere associato all'uso della tecnologia.

Il personale **non deve mai** inoltrare contenuti inappropriati ricevuti da un bambino, un genitore o un membro del personale a un altro bambino, genitore o membro del personale. Se ricevono un contenuto di questo tipo, devono informare immediatamente il DSL/CPC e il responsabile, che chiederanno consiglio al responsabile regionale per la salvaguardia. Il personale non deve cancellare il contenuto fino a quando non viene avvisato

di farlo.

7.8. Internet offre agli utenti opportunità senza precedenti per ottenere informazioni, partecipare a discussioni, collaborare e mettersi in contatto con individui, organizzazioni e gruppi in tutto il mondo, in modo da aumentare le competenze, le conoscenze, la consapevolezza e le abilità.

7.9. La scuola fornisce un accesso adeguato a **Internet e ai social media** per supportare l'istruzione e la gestione dell'attività scolastica.

7.10. La scuola sostiene attivamente l'accesso alla più ampia varietà di risorse informative disponibili, accompagnato dallo sviluppo delle competenze necessarie per filtrare, analizzare, interpretare e valutare le informazioni incontrate. Le parti interessate non devono:

- Utilizzare un dispositivo scolastico o la rete scolastica per visitare intenzionalmente siti Internet che contengono contenuti osceni, illegali, odiosi, abusivi, offensivi, pornografici, estremisti o comunque inappropriati.
- Utilizzare un dispositivo scolastico o la rete scolastica per accedere a siti web di gioco d'azzardo.
- Collegarsi (a qualsiasi titolo) con studenti di età inferiore ai diciannove anni su qualsiasi sito di social network o tramite telefoni cellulari personali o piattaforme professionali. Se ricevono una richiesta di connessione, non devono rispondere (fare riferimento al Codice di condotta).
- Fare commenti offensivi o inappropriati, compreso il discredito del nome e della reputazione della scuola, e/o su qualsiasi genitore o bambino associato alla scuola, su qualsiasi forum/piattaforma, come i siti di social media (sia che si utilizzi un dispositivo della scuola sia che non lo si utilizzi) dove si possa ragionevolmente stabilire un collegamento tra l'utente e la scuola.

Le parti interessate devono:

- Comunicare a un membro dell'SLT, del DSL/CPC o del team di supporto informatico qualsiasi materiale/contenuto inappropriato a cui si è avuto accesso su un dispositivo scolastico o sulla rete della scuola, in modo da poter indagare e bloccare l'accesso in modo tempestivo. Le scuole contatteranno i colleghi del supporto regionale, se necessario
- Riconoscere e rispettare la privacy degli stakeholder sui siti di social media.

8 Dispositivi assegnati Cognita: Accesso e privacy

8.1. Accesso ai dispositivi e ai file digitali (contenuti) assegnati:

- I dispositivi tecnologici scolastici assegnati al personale e agli studenti sono ad uso esclusivo dell'assegnatario.
- I dispositivi 1-to-1 degli studenti possono essere caricati con un'applicazione di gestione dell'aula che consente all'insegnante di controllare e visualizzare lo schermo degli studenti durante la lezione.
- Cognita si riserva il diritto di effettuare ispezioni periodiche del dispositivo per controllare lo stato fisico del dispositivo e per verificare che sia installato solo il software approvato.
- I dispositivi Cognita possono essere caricati con Applicazioni di Supporto Remoto che consentono al personale di supporto IT di accedere ai dispositivi per fornire assistenza remota; ciò può essere utilizzato solo con il permesso dell'assegnatario del dispositivo e il personale di supporto IT si disconnetterà dal dispositivo una volta terminata la sessione.
- Cognita si riserva il diritto di accedere a un dispositivo assegnato e di monitorarne l'uso e il contenuto nelle seguenti circostanze speciali, tra cui, ma non solo:

- Individuare e/o prevenire i reati
- Per consentire la protezione della sicurezza del sistema (ad esempio, virus, malware, hacking o qualsiasi altro rischio).

- Per indagare su potenziali usi impropri, abusi e/o attività illegali.
- Indagare sui problemi di salvaguardia
- Monitorare il rispetto degli obblighi occupazionali e statutari
- Garantire l'integrità dei dispositivi e dei sistemi informatici della scuola.

- Per accedere a un dispositivo assegnato, è necessario fornire un'autorizzazione scritta come segue:

  - Cognita HR Director o Partner per un dispositivo assegnato a un membro del personale
  - Il Direttore della scuola per un dispositivo assegnato a uno studente

- I dati presenti su un dispositivo Cognita o a cui si accede attraverso un dispositivo Cognita sono regolati dalle Politiche sulla Privacy di Cognita e della Scuola.
- Nelle indagini di salvaguardia, può essere necessario l'accesso completo e immediato al dispositivo dello studente/membro del personale. Questa operazione può essere completata senza autorizzazione scritta quando si teme che uno studente/altro possa essere a rischio di danni. L'accesso può essere effettuato solo da un membro del team di salvaguardia, il responsabile, con il supporto dell'IT regionale, se necessario. *Si prega di notare che l'accesso non diretto sarà effettuato su base regolare per intraprendere controlli di monitoraggio (vedere 4.4).

9 Fotografie e immagini

9.1. La scuola rispetta la legislazione in materia di protezione dei dati, in particolare il Regolamento generale sulla protezione dei dati del 2018 (come modificato, ampliato o rielaborato di volta in volta) e le normative specifiche dei singoli Paesi, ed è consapevole che un'immagine o un video di un soggetto è considerato un dato personale sensibile. Chiede il consenso scritto per scopi con finalità esclusivamente pedagogiche, didattiche e documentali per far conoscere le attività svolte alla all'interno della comunità scolastica e del Gruppo Cognita, come ad esempio allestimento ambienti scolastici, allestimento di mostre, proiezioni per le famiglie della scuola, pubblicazioni e newsletter interne, comunicazioni inviate alle famiglie tramite l'applicazione Cognita Connect o altri applicativi di comunicazione interna alla scuola. Chiede specifico consenso scritto dei genitori per la pubblicazione di immagini o video per scopi pubblicitari o di marketing esterni (uso immagini a scopo commerciale), come il sito web della scuola. I genitori, i tutori e gli studenti dai 14 anni in su (art. 2 d.lgs.196/2003 e s.m.i., cd. Codice privacy) possono revocare tale consenso in qualsiasi momento tramite il modulo "Utilizzo delle immagini" e/o informando per iscritto l'Amministrazione della scuola.

9.2. Il Codice di condotta per il personale di Cognita afferma che "Cognita **non** consente l'uso di telefoni cellulari personali, dispositivi intelligenti e macchine fotografiche da parte del personale in presenza di studenti".

9.3. I dispositivi personali **non devono mai** essere utilizzati per scattare, conservare o condividere immagini degli studenti.

9.4. Gli interessati non possono utilizzare dispositivi di lavoro come telefoni cellulari, macchine fotografiche o registratori digitali per fotografare o registrare membri del personale o studenti senza il loro permesso scritto (nel caso di studenti di età inferiore ai 14 anni, il permesso deve essere richiesto per iscritto ai genitori).

9.5. I genitori sono invitati a fare attenzione quando riprendono video o fanno fotografie durante gli eventi scolastici e sono invitati a non pubblicare materiale di altri studenti in qualsiasi forum pubblico senza

l'autorizzazione della famiglia interessata.

9.6. È illegale vendere o distribuire le registrazioni degli eventi senza autorizzazione. I genitori che non desiderano che il proprio figlio sia ripreso o fotografato da altri partecipanti agli eventi scolastici devono informare la scuola in anticipo e per iscritto.

10 Uso di attrezzature scolastiche per uso personale

10.1. I dispositivi scolastici e i sistemi informatici sono forniti solo per il lavoro scolastico e per scopi commerciali; se un membro del personale decide di utilizzare le attrezzature e/o i sistemi informatici per uso personale, si prega di essere informati che ciò avverrà a suo esclusivo rischio e potrebbe essere considerato una violazione della presente Policy Informatica. Inoltre, come previsto dalla Sezione 8 della presente Policy, Cognita ha il diritto di accedere e monitorare l'uso e il contenuto delle attrezzature e della tecnologia della scuola, comprese le comunicazioni personali che possono essere state effettuate attraverso tali mezzi scolastici.

10.2. Solo software e applicazioni approvati possono essere installati su un dispositivo Cognita o utilizzati tramite un browser, come previsto dal processo di Data Privacy Impact Assessment (DPIA) di Cognita. Per saperne di più su questo processo, cliccate qui. Un elenco di software e applicazioni approvati (nonché non approvati e in attesa di approvazione) è disponibile qui. Per saperne di più sulla DPIA, fate riferimento alla sezione 14 di questa policy.

10.3. I dispositivi e le reti scolastiche **non devono** essere utilizzati per svolgere attività illegali.

10.4. Il personale **non** deve effettuare transazioni private o finanziarie sulle apparecchiature condivise, poiché queste comportano il rischio di una violazione dei dati.

11 Uso di attrezzature personali a scuola

11.1. I dispositivi personali **non devono** essere collegati alla rete scolastica, se non alla rete Wi-Fi degli ospiti e con l'autorizzazione della direzione della scuola.

11.2. I dispositivi personali non devono essere utilizzati in presenza di bambini (vedere paragrafi 9.2 e 9.3).

12 Procedura per la segnalazione di problemi e incidenti

12.1. Gli stakeholder possono nutrire preoccupazioni in merito a quanto segue, per quanto riguarda la tecnologia:

- uso non sicuro e/o inappropriato
- accesso a materiale/contenuti non idonei
- minaccia di virus/malware o altre attività dannose, compreso l'hacking
- perdita, danno o furto*

*Ogni caso di furto deve essere denunciato alla Polizia e deve essere ottenuto un numero di riferimento del crimine che deve essere condiviso con un membro dell'SLT e con l'IT regionale.

Tutti i problemi e gli incidenti devono essere segnalati al Cognita Service Desk: servicedesk@cognita.com o via Italia: +39055093073 REGNO UNITO: +44 3301244417; Spagna +34936296806;

12.2. Per qualsiasi problema o incidente di questo tipo è necessario adottare le seguenti misure:

- Interrompere il problema e/o rimuovere la tecnologia (a meno che ciò non comprometta

un'indagine interna o quella di un'agenzia esterna, ad esempio la polizia).

- Impedire l'esposizione dell'incidente ad altri
- Segnalare l'incidente o la preoccupazione a un insegnante, al capo d'istituto, al DSL/CPC o al team di supporto informatico, a seconda dei casi. Se la situazione è complessa e grave, il Direttore della scuola deve riferire la questione al responsabile regionale della salvaguardia e/o al responsabile europeo dell'IT.
- Registrare la natura dell'incidente e le persone coinvolte utilizzando i moduli appropriati, come e quando richiesto.
- Conservare le prove per consentire eventuali indagini, se necessario.

12.3. Il personale **non deve** svolgere indagini prima di essere stato autorizzato dal responsabile, dal responsabile regionale della salvaguardia e/o dal responsabile europeo dell'IT.

12.4. Il responsabile/DSL/CPC o un altro membro del personale designato deve compilare un modulo di segnalazione di incidente grave (SIRF), come indicato dal responsabile della salute e della sicurezza/responsabile regionale della salvaguardia, dopo qualsiasi indagine.

12.5. Il personale deve riferire a un membro dell'SLT o al DSL/CPC quando:

- sono testimoni o sospettano l'accesso a materiale/contenuti non idonei da parte degli stakeholder
- siano testimoni o sospettino che le chat di Teams siano utilizzate per disturbare l'apprendimento o per creare fastidio al personale o agli studenti.
- sono in grado di accedere a materiale/contenuti non idonei
- insegnano argomenti che potrebbero creare un'attività insolita sui log di filtraggio
- si verifica un guasto nel software e/o un abuso del sistema
- si percepiscono restrizioni irragionevoli che incidono sull'insegnamento e sull'apprendimento o sui compiti amministrativi
- si accorgono di abbreviazioni o errori ortografici che consentono l'accesso a materiale riservato

12.6. L'accesso a materiale non adatto e le preoccupazioni relative a virus e altri software dannosi su un dispositivo scolastico o sulla rete della scuola devono essere segnalati a un insegnante, a un membro del team di gestione della scuola o al team di assistenza informatica non appena possibile e nello stesso giorno.

12.7. Lo smarrimento, il danneggiamento o il furto della tecnologia scolastica devono essere segnalati a un insegnante, a un membro del team di gestione della scuola o al team di supporto informatico non appena possibile e nello stesso giorno; il furto deve essere segnalato anche alla polizia e deve essere ottenuto un riferimento di reato (vedi sopra).

12.8. Gli studenti devono assumersi la responsabilità dell'uso delle apparecchiature informatiche sia a scuola che a casa; se i genitori o i tutori dovessero avere dei dubbi o venire a conoscenza di un problema, incoraggiamo vivamente a comunicare tempestivamente con la scuola in modo da poter offrire consigli e supporto.

12.9. La scuola ha il dovere di riferire alle autorità (assistenza sociale/servizi sociali) o alla polizia, in linea con i requisiti di legge, le gravi preoccupazioni relative alla salvaguardia dei soggetti interessati (vedere la Policy di salvaguardia).

13 Rimozione dell'accesso alla rete, degli account e dei dispositivi

13.1. Chiunque venga sorpreso a violare la Policy IT può vedersi revocare l'accesso alla rete, l'account o il dispositivo e può essere soggetto a ulteriori azioni disciplinari.

13.2. La scuola e l'IT regionale si riservano il diritto di rimuovere l'accesso alla rete in qualsiasi momento.

13.3. La scuola può informare la polizia o altre autorità preposte all'applicazione della legge in caso di utilizzo che possa essere considerato come causa di un procedimento penale.

13.4. La scuola prende sul serio le proprie responsabilità in relazione alla sicurezza digitale e all'uso della tecnologia da parte degli stakeholder e comprende l'importanza di monitorare, valutare e rivedere regolarmente le proprie politiche e procedure.

14 Valutazione dell'impatto sulla privacy (DPIA)

14.1. Cognita esegue una DPIA su applicazioni, siti web, software e servizi, collettivamente "terze parti", in cui vengono raccolti dati personali. Questo per garantire che la terza parte possa essere affidabile con le nostre informazioni, in particolare quelle relative ai minori. Per saperne di più su questo processo, cliccate qui.

Le parti interessate devono:

- utilizzare solo terze parti approvate - consultare l'elencoqui
- limitare la quantità di dati personali divulgati a terzi (condividere solo le informazioni necessarie per il funzionamento del prodotto/servizio)
- rispettare le condizioni d'uso della terza parte. Spesso (ma non sempre) ciò comprende quanto segue:
    - una restrizione di età (nel caso di applicazioni, siti web e software destinati agli studenti, spesso, ma non sempre, si tratta di 13 anni)
    - consenso da parte di un adulto idoneo (ad esempio, insegnante, genitore e/o tutore) per l'utilizzo da parte del minore del prodotto/servizio di terzi
    - una richiesta da parte di un adulto appropriato (ad esempio, insegnante, genitore e/o tutore) di creare un account per il minore

Le parti interessate **non devono**:

- partecipare a forum online/pubblici che possono essere presenti in un'applicazione e/o in un sito web
- interagire con utenti sconosciuti tramite un'applicazione e/o un sito web
- utilizzare terze parti non approvate e/o in attesa di approvazione, a meno che non siano autorizzate per iscritto
- utilizzare licenze personali per accedere a servizi di streaming televisivo e musicale
- riprodurre contenuti da piattaforme di streaming multimediale se non si è in possesso di una licenza/autorizzazione da parte del titolare dei diritti

15 Intelligenza artificiale (AI)

15.1. Si rimanda alla **Dichiarazione Cognita sull'Intelligenza Artificiale nell'**Educazione**
**A partire da ottobre 2024, questa dichiarazione è in fase di rielaborazione. La policy informatica regionale sarà aggiornata dopo la rielaborazione e i lettori saranno indirizzati alla dichiarazione tramite un link.

16 Porta il tuo dispositivo (BYOD)

Cognita comprende l'importanza della tecnologia e dell'accesso online per sostenere gli obiettivi di insegnamento e apprendimento. Tuttavia, la necessità di accedere ai contenuti online deve essere bilanciata con la sicurezza online dei nostri stakeholder, in particolare dei nostri studenti.

BYOD è la pratica di consentire agli individui di portare i propri dispositivi tecnologici (personali) sul posto. A partire da giugno 2024, la posizione BYOD di Cognita si differenzia tra personale e studenti:

16.1. Il personale può portare con sé un dispositivo personale in loco, ma **non deve farlo**:

- utilizzare tale dispositivo in presenza di studenti
- collegare il dispositivo alla rete scolastica, ma solo alla rete WIFI degli ospiti.
- non svolgere attività lavorative sul proprio dispositivo personale

16.2. Gli studenti **non devono** utilizzare un dispositivo personale sul posto a meno che non abbiano un'autorizzazione *scritta* da parte di un membro dell'SLT e/o dell'IT regionale. Gli studenti devono avere un motivo eccezionale per non utilizzare il dispositivo fornito dalla scuola.

Durante l'anno accademico 2024-25, Cognita esplorerà il BYOD nel contesto degli studenti e avvierà una sperimentazione BYOD in alcune delle nostre scuole. Tale sperimentazione determinerà la futura posizione di Cognita in termini di BYOD per gli studenti.

17 Comunicazione online e messaggi istantanei

17.1. Per proteggere gli studenti da comunicazioni dannose e/o inappropriate, Cognita ha posto delle restrizioni su alcuni canali di comunicazione. Queste sono impostate per impostazione predefinita, ma possono essere modificate per le singole scuole e/o per gli studenti su richiesta del Direttore della Scuola e con l'approvazione del Responsabile IT Regionale. Si prega di vedere la tabella sottostante che delinea ciò che è/non è disponibile per gli studenti, per impostazione predefinita:

Email			MS Teams	
Inviare all'esterno*	**Ricevere esternamente**	**Inviare / ricevere tra le scuole Cognita**	**Funzione di chat**	**Pubblicare in un Canale squadre (di cui sono membri)**.**
✓	✗	✗	✗	✓

*Per chiarire, gli studenti che inviano e-mail esterne devono avere l'autorizzazione scritta dell'SLT e un insegnante come cc nella loro e-mail in uscita.

Per chiarire, gli studenti possono e devono lasciare messaggi in Teams solo negli spazi creati e gestiti dagli insegnanti. Gli studenti **non devono creare squadre in MS Teams.

18 Appendice A - Dichiarazione sul filtraggio del Web

La dichiarazione che segue fornisce i dettagli delle disposizioni in atto per il filtraggio e il monitoraggio dell'utilizzo all'interno delle scuole Cognita.

Tutto l'utilizzo di Internet all'interno della scuola è filtrato e monitorato. Tutto il traffico di rete viene indirizzato tramite DNS a Cleanbrowsing, una soluzione di filtraggio SafeSearch basata su cloud. Cleanbrowsing fornisce misure di protezione che bloccano o filtrano l'accesso a Internet a immagini che sono: (a) oscene; (b) pedopornografiche; o (c) dannose per i minori. Per impostazione predefinita, Google Chrome e Microsoft Edge sono impostati in modalità sicura. I domini dannosi e di phishing sono bloccati. Il filtro di sicurezza blocca l'accesso ai domini di phishing, spam, malware e maligni. Il database dei domini dannosi viene aggiornato ogni ora ed è considerato uno dei migliori del settore.

Tutto il traffico di rete è sottoposto a filtraggio web da parte di Smoothwall, Watchguard o Fortinet Firewalls. Politiche specifiche di filtraggio del web sono applicate a gruppi diversi per ogni scuola (ad esempio, personale, 6° modulo, fasi chiave 1-4). Smoothwall analizza il traffico in base a una serie di criteri configurati per la scuola e consente o blocca l'accesso ai siti web in base alla loro categorizzazione e al loro contenuto.

Su tutti i dispositivi 1to1 degli studenti è installato un agente di filtraggio web Lightspeed che utilizza un'intelligenza artificiale avanzata per bloccare automaticamente milioni di siti, immagini e video inappropriati e dannosi.

Smoothwall, Fortinet, Watchguard e Lightspeed registrano le attività per l'analisi, le indagini e i rapporti. L'analisi del traffico e dell'utilizzo di Internet viene valutata periodicamente per aggiornare le regole di filtraggio.

Ulteriori dettagli sulle risposte dei fornitori di monitoraggio Lightspeed, che evidenziano fino a che punto il nostro strumento di filtraggio blocca i contenuti dannosi e inappropriati, senza impattare in modo irragionevole sull'insegnamento e sull'apprendimento: https://www.lightspeedsystems.com/media-release/lightspeed-systems-gains-uk-safer-internet-centre-accreditation/

Il responsabile regionale per la salvaguardia è disponibile a fornire assistenza per qualsiasi questione relativa alla salvaguardia che richieda un'escalation.

I membri del Cognita Regional IT Team sono disponibili a fornire supporto per le questioni che richiedono un'escalation.

Contatti chiave:

- Cognita Responsabile IT - Europa e Stati Uniti
- Responsabile regionale per la salvaguardia
- Responsabile del Gruppo per la sicurezza informatica

Appendice B - Modulo di consenso per iPad/Laptop 1-to-1 degli studenti

ACCORDO PER L'UTILIZZO DI iPAD/LAPTOP DA PARTE DEGLI STUDENTI 1-a-1

- L'iPad/laptop sarà parte integrante dell'esperienza di apprendimento a scuola.
d'ora in poi. Trattatelo con cura e usatelo per collaborare con i vostri insegnanti e compagni di classe
in modo mirato per sostenere il vostro percorso di apprendimento. Abbiamo elencato alcune semplici linee guida
per aiutarvi a essere sicuri e responsabili quando utilizzate il vostro dispositivo 1-to-1. Si prega di leggere
e impegnatevi a prendervi cura del vostro dispositivo e a mantenere voi stessi e i vostri compagni di classe
compagni di classe mentre lavorate nell'ambiente virtuale.

ESSERE SICURI

- Visitate solo i siti web che supportano gli obiettivi di apprendimento assegnati dai vostri insegnanti.
- Parlate con i vostri compagni di classe sul vostro dispositivo per collaborare ai compiti di apprendimento e ricordate di
impegnarsi sempre con gli altri come se la conversazione avvenisse faccia a faccia. Siate gentili e
rispettoso in ogni momento.
- Il vostro dispositivo è dotato di tutte le applicazioni e i software necessari per l'apprendimento e il lavoro.
efficacemente. Non è consentito installare applicazioni o modificare le impostazioni a meno che l'insegnante non lo
abbia richiesto.

ESSERE RESPONSABILI

- Tenete al sicuro il vostro iPad/laptop quando siete in viaggio.
- Chiudete a chiave l'iPad/laptop quando non è con voi o conservatelo in un luogo sicuro.
- Maneggiare l'iPad/laptop con cura, tenendolo lontano da cibo e liquidi.
- Segnalare eventuali danni o problemi all'insegnante di classe.
Non utilizzare inchiostro permanente, adesivi o qualsiasi altra sostanza abrasiva che possa segnare o danneggiare il dispositivo.

Mi impegno a prendermi cura del mio iPad / Laptop mantenendolo al sicuro, e ad essere sempre responsabile e rispettoso degli altri nelle mie parole e azioni quando lo uso.

Nome:

Data:

19 Appendice C - Politiche correlate

Europa e Stati Uniti Stati

Consultare le politiche relative sul sito web della scuola www.florencebilingualschool.it come la Policy di salvaguardia e protezione dei minori e la Policy del Codice di condotta.

Commentato [JB2]: Includere i link alle politiche pertinenti

Gruppo IT

- Criteri di gruppo - Software (applicazioni)
- Policy della password Cognita.pdf
- Cognita_Cyber_Security_Policy.pdf
- Sistemi di Salvaguardia Cognita_Policy di Sicurezza Informatica

20 Appendice D - Risorse online correlate "solo guida".

Dipartimento dell'Istruzione (DfE)

- Mantenere i bambini sicuri nell'istruzione (KCSIE)
- Soddisfare gli standard digitali e tecnologici nelle scuole e negli istituti superiori
- Protezione dei dati nelle scuole
- Il dovere di prevenzione

Ufficio del Commissario per l'Informazione (ICO)

- Valutazione d'impatto sulla protezione dei dati

Rete di Londra per l'apprendimento (LGfL)

- Audit sulla sicurezza online

Griglia di apprendimento del sud-ovest (SWGfL)

- Strumento di autovalutazione della sicurezza online per le scuole

Centro nazionale di sicurezza informatica

- Formazione sulla sicurezza informatica per il personale scolastico

Altro

- Centro britannico per l'uso sicuro di Internet
- Resilienza digitale

Proprietà e consultazione	
Sponsor/approvatore del documento	Responsabile IT - Europa e Stati Uniti
Autore del documento	Responsabile IT - Europa e Stati Uniti
Consultazione con	Consulenti per l'apprendimento digitale in Europa
	Gruppo Sicurezza informatica
	Europa IT POD Leads
	Responsabile regionale della salvaguardia (Europa e Stati Uniti)
Pubblico	
Pubblico	Dipendenti regionali
	Studenti e genitori regionali
	Fornitori
	Visitatori
	Appaltatori
Applicazione del documento	
La policy è legata a questa giurisdizione	Tutte le scuole e gli uffici Cognita Europa e Stati Uniti
Controllo della versione	
Ciclo di revisione	Annuale
In vigore da	Settembre 2024
Data della prossima revisione	Settembre 2025
Versione	1.0 EMESSO