COGNITA

Europe IT Policy

September 2026

Cognita Schools Limited No 02313425. Registered Office: Seebeck House, One Seebeck Place, Knowlhill, Milton Keynes MK5 8FR

Contents

1 Introduction....3
2 Policy Purpose....3
3 Policy Scope....4
4 Roles and responsibilities....4
5 Safe Use of Technology....5
6 The Right to Use School and Office Network and Equipment....7
7 Appropriate Use of Technology for Digital Safety....8
8 Cognita Allocated Devices: Access & Privacy....11
9 Photographs and Images....11
10 Use of School Equipment for Personal Use....12
11 Use of Personal Equipment for School or Work....13
12 Procedure for Reporting Concerns and Incidents....13
13 Removal of Network Access, Accounts and Devices....15
14 Retrieval of Personal Files for Former Employees....15
15 Data Privacy Impact Assessment (DPIA)....16
16 Websites and Filtering....16
17 Artificial Intelligence (AI)....17
18 Bring Your Own Device....17
19 Online communication and instant messages....17
20 Monitoring students' online activity (including emails and chat)....20
21 Use of drones....20
22 Smart devices and user tracking....21
23 Appendix A - Web Filtering Statement....23
24 Appendix B - Student 1-to-1 iPad/Laptop Consent Form....24
25 Appendix C – Parent disclaimer for communicating via Microsoft (MS) Teams....25
26 Appendix D - Related Documentation....26
27 Appendix E - Related Online Resources....26

1 Introduction

The use of technology as a tool and enabler has become an integral part of school and home life. Cognita is committed to the effective and purposeful use of technology for teaching, learning and administration and is fully committed to protecting its staff (including contractors and peripatetic teachers), students, parents and visitors, collectively "stakeholders" from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.

Cognita actively promotes the participation of parents to help the school safeguard the welfare of students and promote the safe use of technology.

This policy applies to the use of IT equipment, applications, and services collectively "technology" (both on and off-site) that is supplied and/or made available to stakeholders via the school and/or regional office networks.

A copy of this policy is available on request and posted on the schools' websites.

In the event of a breach of this policy, failure to have read this policy will not be accepted as a defence by any stakeholder. In such cases, Cognita reserves the right to investigate and take necessary action.

2 Policy Purpose

2.1 Promote a culture of responsible behaviour, safe use of, and care for any technology available to stakeholders in both schools and regional offices (whether on or off-site).

2.2 Outline the acceptable and unacceptable use of technology in schools and regional offices (both on and off-site).

2.3 Outline the main roles and responsibilities of all stakeholders when using Cognita technology.

2.4 Educate and encourage students to make good use of the educational opportunities presented by access to technology at their school.

2.5 Safeguard and promote the welfare of students, in particular, by anticipating and preventing the risks arising from:

- Deliberate or unintended exposure to harmful and/or inappropriate content such as pornographic, racist, extremist and/or other offensive content
- Inappropriate contact from known adults outside of school and/or from strangers
- Inappropriate conduct around the use of technology
- Cyber-bullying and/or online abuse
- Copying and sharing of personal data
- Commercial related concerns and risks; e.g. fraud, scamming, and/or extortion

2.6 Outline process and requirements for reporting misuse of technology and incidents.

2.7 Ensure arrangements are in place for all stakeholders to keep them safe and secure.

3 Policy Scope

3.1 This policy applies to all stakeholders in Cognita Europe schools and offices.

3.2 Schools will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware, software and services associated with them including but not limited to:

- The school network, WIFI and internet access
- Hardware and digital devices, including 'Smart' and (Internet of Things) IOT devices
- Software
- Communication and collaborations applications (e.g. email, Microsoft Teams, WhatsApp, Snapchat)
- Virtual Learning Environments
- Social media (e.g. Facebook, Instagram, Tik Tok, X.com)

This policy applies to any member of the school community where the culture or reputation of the school and/or stakeholders are put at risk by their behaviours or actions.

4 Roles and responsibilities

This policy document is the responsibility of the Cognita Europe & United States Head of IT who shall ensure that technology is deployed and monitored in line with this policy as well as other relevant policies.

4.1. The Managing Directors of each cluster of schools and School Heads are responsible for publishing this policy and its ongoing implementation and monitoring at a school level.

4.2. All stakeholders are responsible for adhering to the policy.

4.3. The Head of Cybersecurity is responsible for the cyber services in line with global Cognita Policy, including Cyber Controls and Web Filtering and Monitoring process.

4.4. The Designated Safeguarding Lead (DSL), known as the Child Protection Co-ordinator (CPC) in Spain, is responsible (with the delegated support of deputies/and or IT colleagues) for having an overview of safeguarding and online safety. This includes (but is not limited to):

- Monitoring student's online activity and completing records of this (further details in Appendix A – Web Filtering Statement)
- Following up on safeguarding concerns related to digital communication or all IT related matters concerning students, their parent(s) or carer(s) and external agencies as required (further details in Cognita's Safeguarding Policy)
- Raising any concerns in relation to monitoring devices and/or results of this with regards to individual students with the Regional Safeguarding Lead (who will escalate as needed to the Europe and United States Head of IT if the matter involves a technology component)
- Ensuring that staff are trained in terms of online safety for children, and how to

recognise risks and any indicators of concern
- Ensuring that children are taught how to keep themselves safe online, and the potential risks around online activity

5 Safe Use of Technology

5.1. The school is committed to the safe and purposeful use of technology for teaching, learning, and administration.

5.2. Use of technology must be safe, responsible, respectful to others, and legal. Stakeholders are responsible for their actions, conduct and behaviour when using technology at all times.

5.3. The school will support the use of technology and make internet access as unrestricted as necessary, whilst balancing the educational needs, safety, and welfare of relevant stakeholders, as well as the security and integrity of our systems.

5.4. Monitoring, logging, and alerting tools are in place to maintain technology safety, safeguarding, and security for the protection of stakeholders.

5.5. The filtering and monitoring tools are reviewed centrally on an annual basis to ensure that the current provision addresses all needs of our staff and students. This review involves colleagues in IT, Cyber Security, and Safeguarding, as well as Governors and Proprietors.

5.6. In the interest of safeguarding students, student 1-to-1 devices have monitoring software pre-installed which blocks certain sites and provides live and historic data regarding the device usage e.g. web browsing. The data collected is stored for up to a 90-day period.

5.7. The monitoring software uses Artificial Intelligence (AI) to determine how new websites are filtered and which categories their content falls within (further details in Appendix A).

5.8. IT Support and IT Management have the authority to make manual changes within the filtering system in schools provided they have approval from the School Senior Leadership Team (SLT) and/or Regional IT.

5.9. The school safeguarding team is responsible for having an oversight of the monitoring systems and processes in place. Safeguarding teams in school regularly monitor student's use of school devices, prioritising vulnerable students, whilst also undertaking random checks where operationally possible. Training is available to support staff to understand how to analyse the filtering data within the Lightspeed system.

5.10. All staff, and those with governance oversight, have annual cybersecurity awareness training.

5.11. All staff should understand the expectations and responsibilities related to the filtering system. All staff should understand that the filtering system is in place to safeguard students from harmful online content including that related to (but not limited to) pornography and mature/adult content, radicalisation, violence, hate and racism, criminal activity and terrorism*. The appropriateness of any filtering and monitoring systems are a matter for individual schools and will be informed in part, by the risk assessment required by the Prevent Duty (UK).

**In line with the UK Government strategy to stop individuals from becoming terrorists and/or supporting terrorism otherwise known as Prevent.*

5.12. The school can request that bespoke changes to block/unblock websites are made for their school and shall be requested via the Cognita Service Desk or their IT Manager.

5.13. The school must not use alternative filtering systems. All filtering, whitelisting, blacklisting and testing is regularly undertaken by the Regional IT team who are responsible for making sure that the school's web filtering system(s) are effective.

5.14. It is each school's responsibility to educate students about the importance of safe and responsible use of technology to help protect themselves and others online. Regional IT and the Digital Learning Team support this via various resources (including this one) and training.

5.15. Cognita encourages feedback and participation from parents, for example, via the 'Voice of the Parent' (VoP) survey, to help promote the safe and effective use of technology for students to progress their learning and skills.

5.16. Any concern regarding unsafe or inappropriate use of technology must be reported to a member of the SLT, Head of School or DSL/CPC or Cognita's Service Desk on the same day of the identification of the concern.

5.17. Any serious incident involving unsafe or inappropriate use of technology must be reported immediately by the Head School and/or DSL/CPC to the Cognita Europe and United States Head of IT (for technology matters) and to the Regional Safeguarding Lead (for safeguarding matters) who will work with relevant colleagues to record, investigate and mitigate risks related to the incident. When directed to do so, a Serious Incident Referral Form (SIRF) must be completed by the school, following their investigation and interventions with support from Regional IT and Safeguarding colleagues.

5.18. All users of technology may find the following resources helpful in keeping themselves and others safe online:

- UK Safer Internet Centre
- Internet Matters - resources
- Google Family Safety
- Common Sense Media

In addition, schools shall meet the Cyber security standards set by the government and/or local authorities.

To support schools to meet this duty, the UK Department for Education has published filtering and monitoring standards which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and/or inappropriate content (e.g. explicit images, violent or hateful content, and other forms of harmful media) without unreasonably impacting teaching and learning

- Have effective monitoring strategies in place that meet their safeguarding needs.

Whilst there isn't a single EU equivalent as specific and prescriptive as the UK DfE filtering and monitoring standard, there are European-level frameworks and guidance such as:

Digital learning and ICT in education | Shaping Europe's digital future

Home - Better Internet for Kids

6 The Right to Use School and Office Network and Equipment

6.1. School employees and students will be allocated a username and password for accessing technology devices and services. They must **not** allow other individuals to use their account and shall not share any passwords with anyone.

6.2. School email accounts should only be accessed through Cognita's Microsoft Office 365 and all other third-party email services are **not** allowed.

6.3. Some shared resources (available in school and offices for use by employees and students) will have a generic username and password for access and is managed by the teacher.

6.4. All school technology remains the property of Cognita. The school may reasonably request the device or withdraw access to the service, for any student, at any time and, if applicable, the device must be returned to the school by the student.

6.5. Only school devices must be connected to the school network and personal devices should only connect to the guest network; if allowed by a member of the school SLT.

6.6. Staff's personal devices must not be used for work related tasks in the school and must never be used where students are present.

6.7. Any attempt to access or use any account, email address or IT resource belonging to another stakeholder is prohibited, unless that attempt is made by Regional IT for legitimate business reasons and/or has been authorised via an 'Access to Mailbox and Files Request Form' to the Cognita Service Desk.

6.8. Designated devices may be issued to school employees and students for teaching, learning and administration:

- Students assigned a 1-to-1 device are required to sign the iPad/Laptop Usage Agreement (link in the Appendix B)
- Students with a designated 1-to-1 device may use this in lessons at the direction of their teacher
- Parents are responsible for the cost of a 'repair' or 'like for like' replacement of an assigned device (as directed by the school), if it is damaged / lost intentionally, willfully or through neglect. This is clarified in the schools' Parent Agreement
- Cognita employees and students are responsible for the safety and security of their assigned device at all times

- Cognita issued devices and associated peripherals should be returned in good condition (excluding ordinary wear and tear) and in working order when a stakeholder finishes their time as a student or staff member
- Damaged and/or defective staff devices are replaced, and the costs are covered centrally

7 Appropriate Use of Technology for Digital Safety

7.1. The school provides **System and Application Accounts** for stakeholders for educational and administrational purposes.

7.2. Stakeholders must **not**:

- Allow anyone to use their account unless authorised (in writing) by SLT and/or the Regional IT Team
- Use someone else's account
- Leave their device unlocked and/or logged into their account when not in use
- Use mobile messaging apps to communicate with parents, and/or staff with students
- Send messages and/or emails from school accounts that purport to come from an individual other than the person actually sending the message, unless approved by a member of the school SLT
- Send/store work related information, including messages and ("communication"), and/or personal data to/from a personal account/storage facility.

7.3. The school provides **Hardware and Software** to support education and the running of the school operation.

- Users of school technology equipment are expected to take care of the equipment through responsible behaviour.
- School technology must **not** be removed from school site except where:
    - The device is assigned to an individual member of staff; or
    - The device is assigned to a student via the 1-to-1 programme; or
    - There is written permission from a member of the SLT

- School technology assigned to staff and students is the responsibility of the assignee
- Stakeholders must **not** leave portable technology equipment, including school-issued devices unattended unless, such equipment is out of use (either due to fault(s) or simply, logged out of and shutdown) in which case, it must be stored securely
- Loss or damage of school technology must be reported to a teacher, member of the SLT or IT Support Team on the same day
- Theft of school technology must be reported to the Police by a member of SLT and be reported to a teacher, member of the SLT or IT Support Team on the same day with the Police crime reference number
- Deliberate abuse or damage of school technology equipment will result in the person(s) responsible being billed for the full replacement or repair costs of the equipment

Stakeholders must **not**:

- Attempt to install unapproved software or applications onto school devices
- Download or access illegal software and websites on school devices
- Download any software packages from the school network onto portable media or personal devices
- Attempt to copy or remove software from a school device
- Attempt to alter the configuration of the hardware equipment or any accompanying software

7.4. The school provides technology resources for accessing and storing data and has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare of stakeholders (further details in Appendix A - Web Filtering Statement).

Stakeholders must **not**:

- Bypass website filtering systems and/or technology security systems (via 'Tor' browsing, browser extensions and/or VPNs) whilst using school devices whilst on and/or off-site
- Access or attempt to access data for which they are not authorised
- Interfere with digital work belonging to other users
- Share private, sensitive and/or confidential information unless:
    - they have authority to share
    - the method of sharing is secure
    - the recipient is authorised to receive that information
    - there are legitimate business reasons
    - there are legitimate safeguarding reasons

It is the responsibility of technology users when accessing data to be aware of Intellectual Property rights infringement including copyright, trademark, patent, design and moral rights.

7.5. The school endeavours to safeguard and where possible mitigate all **Security** risks associated with technology and will engage and collaborate with Regional IT, if required.

7.6. Concerns regarding any of the following must be reported to the Head or member of SLT who will, as required contact the Regional Safeguarding Lead and/or the Regional IT Team as soon as possible on the same day:

- Access to unsuitable material/content on a school device or on the school network
- Misuse of technology which has caused (or has the potential to cause) harm or abuse to another, including (but not limited to):
    - cyber bullying
    - upskirting
    - creation and/or sharing of self-generated intimate images and/or videos, including those generated using AI e.g. deepfakes
    - creating and/or sharing AI generated material that is, or could be, considered abusive in its nature
    - creating and/or sharing nudes/semi-nudes
    - blackmail
    - online grooming and/or sextortion
- Concerns regarding viruses and other malicious software
- Suspicious emails, links, and/or websites or any other communication

7.7. It is the responsibility of all technology users to ensure the **welfare** of themselves and others both on personal and school devices. Stakeholders must **not**:

- Use their own or the school's technology to bully others online (cyber bullying) or disrupt

the learning of others

- Use their own or the school's technology to make contact or engage with people who they do not know
- Use their own or the school's technology to create, store, or share sexualised and/or any inappropriate/illegal content including images, audio, video and/or text

Stakeholders must:

- Report any concerns regarding welfare associated with the use of technology to a teacher, member of the School Leadership Team or DSL/CPC at the earliest opportunity.

Staff **must never** forward inappropriate content that they have received from a child, parent, or staff member to any other child, parent, or staff member. Should they receive something of this nature, they must notify the DSL/CPC and Head immediately, who will seek advice from the Regional Safeguarding Lead. Staff must not delete the content until advised to do so.

7.8. The internet provides unprecedented opportunities to obtain information, engage in discussions, collaborate and liaise with individuals, organisations and groups worldwide so as to increase skills, knowledge, awareness, and abilities.

7.9. The school provides appropriate access to the **Internet and Social Media** to support education and the running of the school business.

7.10. The school actively supports access to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret, and evaluate information encountered. However, stakeholders must **not**:

- Use a school device or the school network to intentionally visit internet sites that contain obscene, illegal, hateful, abusive, offensive, pornographic, extremist and/ or otherwise inappropriate content
- Use a school device or the school network to access gambling websites
- Communicate or connect with students via personal social media accounts, personal messaging services, or personal mobile devices. This applies to all students under the age of 18, in line with safeguarding guidance. Should they receive a connection request from a student (be it current or former) they must not reply (please refer to the Code of Conduct)
- Make or upload any offensive or inappropriate comments/imagery (i.e. deepfakes), including bringing the school's name and reputation into disrepute, and/or about any other staff member, parent, and/or child associated with the school, on any forum/platform, such as social media sites (whether using a school device or not) where a connection between the user and the school can reasonably be made

Stakeholders must:

- Notify a member of the SLT, DSL/CPC or IT Support Team of any inappropriate material/content that has been accessed on a school device or on the school network so that this can be investigated, and access can be blocked in a timely manner. Schools will contact regional support colleagues, if required
- Recognise and respect the privacy of stakeholders on all web and social media sites

8 Cognita Allocated Devices: Access & Privacy

8.1. Access to assigned devices and digital files (content):

- School technology devices assigned to staff and students are for the sole use of the assignee only
- Student 1-to-1 devices may be loaded with a Classroom Management Application which enables appropriate functionality for the teacher to control and view the students screen during the lesson period
- Cognita reserves the right to carry out periodic device inspections to check the physical state of the device and to verify that only approved software is installed
- Cognita devices may be loaded with Remote Support Applications which enables IT support staff to log on to the devices to provide remote assistance; this may only be used with the permission of the device assignee and IT support staff will disconnect from the device once the session ends

Cognita reserves the right to access an assigned device and monitor it's use and content under the following special circumstances including, but not limited to:

- To detect and/or prevent crime or policy violation.
- To enable system security protection (e.g. Virus, Malware, Hacking or any other Risk)
- To investigate potential misuse, abuse, and/or illegal activity
- To investigate safeguarding concerns
- To monitor compliance with employment and statutory obligations
- To guarantee the integrity of the school devices and IT systems

To access an assigned device, written permission must be given as follows:

- Cognita HR Director for a device assigned to a member of staff
- The School Head for a device assigned to a student

- Data on a Cognita device or accessed through a Cognita device is governed by Cognita & School Privacy Policies.
- In safeguarding investigations, full access may be needed immediately on the student/staff member's device. This may be completed without written permission where there are concerns that a student/other may be at risk of harm. Access can only be undertaken by the Regional Safeguarding Lead, a member of the school safeguarding team, and/or the Head, with support from Regional IT where needed.

*Please note that non-direct access will be made on a routine basis to undertake monitoring checks (see 4.4).

9 Photographs and Images

9.1. The school abides by data protection legislation, namely, the General Data Protection Regulation (GDPR), and understands that an image or video of a data subject is

considered personal data. It seeks written consent from parents to publish images or videos for non-essential purposes (publicity or marketing, such as the school website), and for essential purposes, such as CCTV. Parents, guardians and students of a specified age (depending on local legislation) may withdraw this permission at any time via the 'Use of Images' form and/or by informing the school's Administration Team in writing.

9.2. The Cognita Code of Conduct for Staff and separately, the Safeguarding and Child Protection Policy state that Cognita does **not** permit the use of any personal device capable of capturing or sharing imagery/videos and/or data **in the presence/close vicinity of pupils whether on/off site**: this includes mobile phones, tablets, any smart devices (including, but not limited to; phones, watches, glasses, and rings/jewelry), hearables and wearables.

9.3. Personal devices must **never** be used to take, store, or share images of students.

9.4. The UK Government's Early years foundation stage statutory framework require all UK schools to have a clear policy on the use of mobile phones and devices. Regarding **pupils** and mobile phone use, please see Cognita's Behaviour Policy, as well as the latest Government guidance: Mobile phones in schools.

9.5. Stakeholders are not permitted to use work devices such as mobile phones, cameras or digital recorders to photograph or record members of staff or students without their written permission. In the case of students of a specified age (depending on local legislation) permission must be sought in writing from their parent(s)/guardian(s)). Permission may only be granted by the school in the event of performances/events organised by the school (and clear boundaries will be described).

9.6. Parents/guardians are asked to be considerate when taking videos or photographs at school events (with permission – see above 9.5) and are requested not to publish material of other students in any public forum without the permission of the relevant family.

9.7. It is illegal to sell or distribute recordings from events without permission. Any parent/guardian who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

10 Use of School Equipment for Personal Use

10.1. School devices and IT systems are provided for school work and business purposes. However, we recognise that staff may occasionally use work devices for personal use. Should a member of staff decide to use the equipment and/or IT systems for personal use, please be informed that it will be at their sole risk. Depending on the use, it could be considered as a breach of this IT Policy. For example, browsing websites during non-work time and in the absence of children (e.g. break time, lunch etc) is generally considered acceptable provided that the website is safe and appropriate. Please note, as per Section 8 of this Policy, Cognita is entitled to access and monitor the use and content of the school equipment and technology, including the personal communications that may have been made through those school means.

10.2. Only approved software and applications may be installed on a Cognita device or used via

a browser as per Cognita's Data Privacy Impact Assessment (DPIA) process. To find out more about this process, please click here (internal stakeholders only). A list of approved (as well as unapproved and pending) software and applications can be found here (internal stakeholders only).

10.3. School devices and networks must **not** be used to carry out any illegal activity.

10.4. Staff shall **not** conduct any private or financial transactions on work equipment as these carry a risk of a data breach.

11 Use of Personal Equipment for School or Work

11.1. Personal devices must **not** be connected to the school or office network, other than to the guest WiFi network

11.2. No personal devices must be used in school where children are present (ref. sections 9.2-9.3).

11.3. Personal devices must not be used for school or work purposes – doing so introduces numerous security risks including, but not limited to:

- weaker security controls – via non-compliant device security services
- outdated software - leaving vulnerabilities unpatched and the user at risk
- data leakage/exposure - sensitive work files could be accidentally synced to personal cloud services

Concerns from a data privacy perspective include, but are not limited to:

- Mixing personal and corporate data - making it harder to control where company information goes
- Lost/stolen device risk - if a personal device with company data gets lost, both personal and business data could be exposed.
- Family/shared use - if others use the stakeholder's personal device, they might unintentionally access confidential work materials

12 Procedure for Reporting Concerns and Incidents

12.1. Stakeholders may have concerns regarding the following, in respect of technology:

- unsafe and/or inappropriate use
- access to unsuitable material/content
- threat of viruses/malware or other malicious activity, including hacking
- loss, damage or theft*

*Any case of theft, must be reported to the Police and a crime reference number obtained which must be shared with a member of the SLT as well as Regional IT.

All concerns and incidents should be reported to the Cognita Service Desk:

UK

servicedesk@cognita.com / +44 330 124 4417

Spain:

servicedesk@cognita.com / +34 936 296 806

Italy:
servicedesk@cognita.com / +39 055 093 9073

12.2. Action must be taken against any such concerns or incidents, as follows:

- Stop the problem and/or remove the technology (unless to do so would jeopardise any internal investigation or that from an external agency e.g. the Police/Social Care)
- Prevent exposure of the incident to others
- Report the incident or concern to a teacher, Head of school, DSL/CPC or IT Support Team as appropriate. If the situation is complex and severe, then the Head must report the matter to the Regional Safeguarding Lead, and the Europe and United States Head of IT.
- Record the nature of the incident and those involved using appropriate forms as and when directed
- Preserve evidence to enable any investigation, if required

12.3. Staff must **not** carry out any investigations until they are authorised to do so by the Head, Regional Safeguarding Lead, and/or the Europe and United States Head of IT.

12.4. The Head/DSL/CPC or other nominated staff member must complete a Serious Incident Report Form (SIRF), as and when directed by the Head of Health and Safety/Regional Safeguarding Lead, after any investigation.

12.5. Staff must report to a member of the SLT or the DSL/CPC when:

- they witness or suspect unsuitable material/content has been accessed by stakeholders
- they witness or suspect that Microsoft Teams Chats are being used to disrupt learning or be a nuisance to staff or students
- they are able to access unsuitable material/content
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software and/or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

12.6. Access to unsuitable material and concerns regarding viruses and other malicious software on a school device or on the school network must be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity on the same day.

12.7. Loss, damage or theft of school technology should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity on the same day; theft must also be reported to the Police and a crime reference obtained (see above).

12.8. Students must take responsibility for their use of IT equipment both at school and at home; should parents/guardians have concerns or become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support.

12.9. The school has a duty to report serious safeguarding concerns related to stakeholders to the authorities (Social Care/Services) or to the Police, in line with statutory requirements (see the Safeguarding Policy).

13 Removal of Network Access, Accounts and Devices

13.1. Anyone found breaching this IT Policy may have their network access, account(s), and/or device removed and may be subject to further disciplinary action following investigation.

13.2. The school and Regional IT reserves the right to remove network access at any time.

13.3. The school may inform the Police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

13.4. The school takes its responsibilities in relation to digital safety and use of technology by stakeholders seriously and understands the importance of monitoring, evaluating and reviewing its policies and procedures regularly.

14 Retrieval of Personal Files for Former Employees

14.1. Cognita strongly discourages the storage of personal files on work devices* (please refer to Section 10 “Use of School Equipment for Personal Use," within this policy). However, we acknowledge that this may occasionally occur. As such, it is the responsibility of employees to ensure that any personal files are removed from company systems before their departure.

**Please be aware that all files stored on work devices and/or systems are considered company property.*

14.2. If a former employee is unable to retrieve their personal files and later requires access, the request will be handled on a case-by-case basis and at the sole discretion of Cognita’s HR and IT department. Please note that neither department is obligated to restore account access. The following steps will be followed for file retrieval:

- **File Location**: the former employee must provide clear instructions to HR and IT regarding the file’s location.
- **Data Collation**: requests must be specific and narrow. General or vague requests (e.g., “Everything personal in my mailbox / OneDrive”) will not be accepted.
- **Content Review**: files will be reviewed to ensure that business, confidential, or disputed materials are excluded. Written consent from the former employee will be required before any release.

14.3. In certain circumstances, Cognita may be legally required to refuse or redact file contents. This includes the following scenarios:

- The employee was dismissed for serious misconduct involving IT or data
- Files cannot be clearly separated from business-related data

- The retrieval request is disproportionate in nature
- There is ongoing litigation or investigation
- The request is vague or excessive

Where files are released, this will be done in a safe and controlled way.

15 Data Privacy Impact Assessment (DPIA)

15.1. Cognita performs a DPIA on applications, websites, software and services, collectively "third parties" where personal data is collected. This is to ensure that the third party can be trusted with our information, particularly that of minors, as well as complying with relevant legislation such as the General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 and the EU-AI Act 2024. To find out more about this process, please click here (internal stakeholders only).

Stakeholders must:

- only use approved third parties
- limit the amount of personal data disclosed to the third party (only share information that is required for the product/service to function)
- adhere to the third party's terms of use. This often (but not always) encompasses the following:
    - an age restriction (in the case of applications, websites and software aimed at students, this is often, but not always (depending on local legislation), 13 years old
    - consent from an appropriate adult (e.g. teacher, parent and/or guardian) for the child to use the third-party product/service
    - a requirement from an appropriate adult (e.g. teacher, parent and/or guardian) to create an account for the child

Stakeholders must **not**:

- engage in online/public forums which may feature on an application and/or website
- engage with unknown users via an application and/or website
- use unapproved third parties and/or those pending approval unless it is authorised in writing
- use personal licenses for TV and music streaming services

16 Websites and Filtering

To protect our stakeholders, Cognita uses a web filtering system on all devices that are connected to the network helping to ensure that internet use aligns with our security, compliance, and productivity standards. The web filtering system is designed to:

- **Enhance security** by blocking access to malicious or high-risk websites that may be deemed inappropriate and/or contain viruses, phishing attempts or harmful content

- **Protect sensitive information** by preventing access to sites or services that could lead to data leaks

- **Support compliance** with legal, regulatory, and contractual requirements regarding internet usage and data protection

  Employees are encouraged to use the internet responsibly and in accordance with company policies.

  Requests to unblock websites, including those that have been created by (Cognita) teachers or independent/stand-alone creators are becoming increasingly popular. Whilst allowing students access to such websites can be valuable for learning, it also comes with risks, including, but not limited to:

- **inappropriate links**: external links or embedded media could lead students to unsuitable or unsafe sites.

- **unmoderated and/or social interaction**: if the site has forums, comment sections, or chat functions, it could open doors to bullying, harassment, or inappropriate interactions.

- **malware or vulnerabilities**: if the site is not regularly maintained, it could be hacked and spread malicious content.

  As such, Regional IT will not approve requests for websites where any of the above are identified on said website.

17 Artificial Intelligence (AI)

17.1. Please refer to the **Cognita Group AI Policy**.

18 Bring Your Own Device

18.1. Staff are permitted to bring a personal device on-site but must **not**:

- use that device in the presence of students
- connect that device to a school network, only to the guest WIFI network
- undertake work-related tasks on their personal device

18.2. Students must **not** use a personal device on site unless they have *written* authorisation by a member of the SLT and/or Regional IT. Students must have an *exceptional reason* not to use their school supplied device.

19 Online communication and instant messages

19.1. To protect students from engaging in harmful and/or inappropriate communication, Cognita has put in place restrictions on certain communication channels. These are set by default but can be changed for individual schools and/or students upon request from the Head of School and approval by the Europe and United States Head of IT. Please see the table below which outlines what is/is not available to students, by default:

Email		
Send externally	**Receive externally**	**Send / receive between Cognita schools**
Unavailable	Partially available	Available
Outgoing emails i.e. where students wish to communicate externally,: *1. must have written permission from SLT and the Regional IT Team via a request submitted to the Cognita Service Desk and;* *2. copy a teacher into the outgoing email.*	*-Incoming emails (to students) are blocked by default. However, they may be unblocked where the sender is part of an approved third-party (such as an app/software provider that has passed Cognita's DPIA process).* *Such third-parties may need to email the student to verify their account or, to reset their password.*	

Microsoft Teams		
Chat function	**Post in a Teams channel**	**Calls**
Unavailable	Partially available	Unavailable
Student chats within Microsoft Teams may only be permitted where there is written permission from SLT and the Regional IT Team via a request submitted to the Cognita Service Desk. The calls must only be within Teams created and overseen by teachers.	*Students can and must only post Microsoft Teams messages in spaces that they are a part of, and that are created and managed by teachers.* *Students **must not** create Teams themselves, in Microsoft Teams.*	*Student calls within Microsoft Teams may be permitted provided there is written permission from SLT and the Regional IT Team via a request submitted to the Cognita Service Desk. The calls must only be within Teams created and overseen by teachers.*

19.2. Staff are encouraged to use Cognita's preferred collaboration platform, Microsoft Teams. However, if this option is not viable in certain circumstances, the use of WhatsApp on a work phone is permitted (although not encouraged), provided that staff do not:

- discuss anything confidential or sensitive about pupils, parents and/or colleagues (note, no safeguarding related information must ever be shared over WhatsApp)
- send inappropriate, offensive and/or controversial messages, GIFs and/or memes (even if they are considered a 'joke')
- share personal data and/or commercially sensitive information

- join and/or create WhatsApp groups created by parents/guardians. This includes those who are both parents and/or employees of the school (doing so is considered a conflict of interest).

Whilst there are several benefits to using WhatsApp for work, its usage must align with our data protection policy and general standards around conduct and professionalism. As such, staff must be mindful when using this app on a work phone and only send messages which they would feel comfortable being disclosed. Keep communication professional, respectful and work-related.

NB: As of April 2025, Meta (the parent company of WhatsApp) introduced an integrated AI assistant known as 'Llama 4' within the WhatsApp messaging platform. While this feature is described as "optional", it cannot be removed from the app interface.
Although the use of Llama 4 on work devices is not encouraged, it is not explicitly prohibited, as Cognita currently has no means of disabling the feature. Employees who choose to engage with the AI assistant must do so with caution and in strict compliance with the **Cognita Global AI Policy**.

In respect of online communication between staff and parents, Cognita's preferred and approved platform is Microsoft Teams (MS Teams). We recognise the importance of effective digital communication, especially for remote meetings and discussions between staff and parents. However, this comes with risks, particularly in the evolving landscape of Artificial Intelligence (AI), where recordings and transcripts can be manipulated.

To mitigate these risks and maintain professional standards, the following guidelines must be followed when conducting online meetings with parents.

In the case of MS Teams

- Every effort should be made to use this platform for online meetings or discussions with parents.
- The meeting must be initiated internally by a member of staff, ensuring the initiator (host) retains control over the session.
- MS Teams meetings must be recorded* (using the hosting tool and not third-party products), to provide a verifiable record, if required at a later stage.
- The use of external transcription tools or plug-ins is strictly prohibited. MS Teams' built-in transcription feature is permitted and should be used if transcription is necessary.
- Professionalism must be maintained at all times. For meetings that may involve sensitive or challenging conversations, a second member of staff preferably from the Senior Leadership Team (SLT) should be present to help guide the discussion in a calm and constructive manner.

*Prior to the recording, it is advised that staff read the disclaimer in Appendix C – Parent disclaimer for communicating via Microsoft (MS) Teams.

In the case of other video conferencing platforms

The use of other video conferencing platforms is not permitted unless they are DPIA approved. The above conditions must also be met and if for any reason they cannot be, please notify servicedesk@cognita.com and/or speak to your Regional IT Management Team.

Cognita is aware that some schools use TES' Parents Evening System for online meetings between parents and teachers. As of August 2025, this platform does not provide a transcription service nor any recording capability. Please be mindful of this, as no record of conversations e.g. what was said and by whom, can later be relied upon. This does not mean that such calls can be transcribed and/or recorded via other means – this is prohibited. Cognita is also aware that parents can initiate calls via the platform. Again, this too is prohibited.

20 Monitoring students' online activity (including emails and chat)

Cognita recognises the importance of keeping children safe online. As such, we reserve the right to monitor students' online activity, including their email accounts. This is particularly applicable in cases where unusual, unsafe or inappropriate activity is suspected and/or reported.

Equally, we are also mindful of students' autonomy and their right to data privacy, especially among our older cohort. Therefore, any online monitoring will be conducted in a reasonable and proportionate manner, with clear justification for why such monitoring is taking place. In short, Cognita's objective is to balance the students' privacy with our responsibility (and duty of care) to protect and supervise them online.

This approach also extends to monitoring carried out by parents and guardians. Whilst Cognita cannot govern the nature of supervision outside of school (such as in the home), we encourage parents to carefully consider the circumstances under which they monitor their child(ren)'s online activity, including their email correspondence. Again, such monitoring should be reasonable and proportionate, taking into account the child(ren)'s age, maturity and right to privacy.

21 Use of drones

Drones are becoming increasingly popular in capturing footage on-site. However, drone use must comply with local regulations (please check the regulations for your region) as well as internal process.

Permission must be sought from the Head of Health and Safety – Europe and United States. If permission is given, then a robust risk assessment must be completed.

From a data privacy perspective, every effort should be made to avoid:

- capturing anything identifiable such as (but not limited to):
  - data subjects (people, including their image and/or voice), car registration plates
- flying drones when individuals are on-site

- flying drones near windows/entrances, car parks etc (where identifiable items are more likely to be present)

If a drone is flown when individuals are on-site, then those individuals must be clearly communicated with in advance and made aware of the initiative so that they can either give permission (consent) or, object to being filmed. They must also be given ample opportunity to raise any queries and/or concerns.

If drone footage is captured and stored locally (e.g. on an SD card) and if that footage includes identifiable data, the school must ensure that the SD card is kept safe/secure at all times. It must remain on site, and the footage erased once it has served its purpose.

If the footage is stored on third-party software (e.g. via a cloud solution), then that software must be vetted by Cognita via the Data Privacy Impact Assessment (DPIA) process.

From a security perspective, drones must **not** be used to interfere with school security measures and/or operations, nor be flown in any way that compromises safety and security.

There are also several important health and safety considerations in respect of drone use – please see the **Facilities Management Policy** for more information.

22 Smart devices and user tracking

The use of smart devices is never permitted in the presence of children. Cognita does not condone the use of tracking devices during school hours and/or school activity e.g. school trips and/or after-school clubs. Schools have existing safety and security measures in place to keep students safe whether they are in school or off site.

However, we recognise that as technology develops to allow parents to track child(ren)'s movements via a smart device, some parents may decide to use this functionality more frequently, for example, when their child(ren) are off school premises i.e. on a school trip. It is up to the parents as to whether they use this technology.

Several arguments for this include:

- parents have a right to know where their child(ren) are
- that parents perceive that the technology can help to keep their child(ren) safe(r)
- that the technology gives the parent peace of mind

However, there are several ethical and safety implications which parents may fail to consider before opting to track their child(ren) via a smart device. Ultimately, parents are advised to balance safety against personal freedom but of course, there are many variables such as, but not limited to:

- the children)'s age
- the children)'s cognitive ability, maturity and understanding
- the location e.g. of the school trip (is it particularly remote and/or perceived greater risk

As such, schools may find tracking devices such as Air Tags embedded within students' possessions and/or clothing. In these situations they should speak with the parent and remind them that:

- such technology is not designed to track individuals' movements rather, the item/belonging itself
- that Cognita does not condone the use of tracking devices during school hours and/or school activity e.g. school trips and/or after-school clubs
- That the parents use of the tracker may provide them with a false sense of security; children may remove or change the location of the tracker. They may also lose the item that the tracker is placed within.

Schools may find it difficult to ban the use of tracking devices (except for those embedded on a mobile phone – please see the school's mobile phone policy). However, as for other tracking devices such as Air Tags, schools may find it helpful to point parents/guardians to this article.

23 Appendix A - Web Filtering Statement

The

The statement below provides details of the arrangements in place for filtering and monitoring usage within Cognita schools.

All internet usage within the school is filtered and monitored. All network traffic is routed via DNS to Cleanbrowsing which is a cloud based SafeSearch Filtering solution. Cleanbrowsing provides protection measures that block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors.

By default, Google Chrome and Microsoft Edge are set to Safe Mode. Malicious and Phishing domains are blocked. The security filter blocks access to phishing, spam, malware and malicious domains. The database of malicious domains is updated hourly and is considered to be one of the best in the industry.

All network traffic has web filtering from on-site Firewalls. Specific web filtering policies are applied to different groups per school (e.g. Staff, 6th form, Key Stages1-4). Our Firewalls analyse the traffic against a set of policies that have been configured for the school and will either allow or block website access based on the websites categorisation and content.

All student 1to1 devices have a web filtering agent installed using advanced AI to automatically block millions of inappropriate and harmful sites, images, and videos.

Our web filtering systems record activities for analysis, investigation and reporting. Analysis of traffic and internet usage is assessed periodically to update filtering rules.

Further details on Lightspeed Monitoring Provider Reponses which highlights to what extend our filtering tool blocks harmful and inappropriate content, without unreasonably impacting teaching and learning:
https://www.lightspeedsystems.com/media-release/lightspeed-systems-gains-uk-safer-internet-centre-accreditation/

Regional Safeguarding Lead is available to support with any safeguarding –related issues that require escalation.

Members of the Cognita Regional IT Team are available to support with issues that require escalation.

Key contacts:

- Cognita Head of IT – Europe & United States
- Cognita Regional Safeguarding Lead
- Cognita Group Head of Cyber Security

24 Appendix B - Student 1-to-1 iPad/Laptop Consent Form

STUDENT 1-to-1 iPAD/LAPTOP USAGE AGREEMENT

• Your new iPad/laptop will be an exciting and integral part of the learning experience at school from now onwards. Treat it with care and use it to collaborate with your teachers and classmates in a purposeful way that supports your learning journey. We've listed some simple guidelines below to help you stay safe and responsible when using your 1-to-1 device. Please have a read and make a firm commitment to look after your device and keep yourself and your classmates safe whilst working in the virtual environment.

BE SAFE

• Only visit websites that support the learning goals assigned by your teachers.

• Talk to your classmates on your device to collaborate on learning tasks and remember to always engage with others as if the conversation were happening face to face. Be kind and respectful at all times.

• Your device has all the necessary apps and software required for you to learn and work effectively. You shall not install any apps or change any of the settings unless your teacher has asked you to do so.

BE RESPONSIBLE

• Keep your iPad/laptop safe when you are on the move.

• Lock your iPad/laptop away when it’s not with you or keep in a safe place.

• Handle your iPad/laptop with care keeping it away from food and liquids.

• Report any damage or problems to your Form Teacher.

• Respect that the laptop cameras may only be used for school-related work. Photos and/or videos of fellow students and/or school staff should only be taken with the explicit permission of the people involved.

I agree to take very good care of my iPad / Laptop by keeping it safe, and always be responsible and respectful of others in my words and actions when using it.

Name:

Date:

25 Appendix C – Parent Disclaimer for Communicating via Microsoft (MS) Teams

Disclaimer to Be Read Aloud to Parents Before the Meeting Begins:

"Before we begin, I'd like to let you know that this meeting is being held via Microsoft Teams, which is our preferred video conferencing platform. This is in line with our internal policy, which requires all sessions between staff and parents to take place on Microsoft Teams.

By initiating the call from our side, we're able to maintain appropriate control of the session in accordance with our safeguarding and data protection procedures.

Please also be aware that this meeting will be recorded. The recording, along with an automatically generated transcript, will be stored securely and may be referred to later if necessary. This is done to ensure transparency and to support accurate record keeping.

If you have any concerns about this, please feel free to raise them now before we proceed."

26 Appendix D - Related Documentation

UK

- Safeguarding and Child Protection Policy
- Preventing Radicalisation Policy
- Behaviour Policy
- Code of Conduct Policy
- Student Charter Data Protection Policy
- Early Years – Use of Mobile Phones, Cameras and Devices Policy
- Preventing Extremism and Radicalisation
- Student Media Policy

Group IT

- Group Policy – Software (Applications)
- Cognita Password Policy
- Cognita Cyber Security Policy
- Cognita Safeguarding Systems – Cyber Security Policy
- Group AI Policy

27 Appendix E - Related Online Resources

Department for Education (DfE)

- Keeping children safe in education - GOV.UK
- Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK
- Data protection in schools - Guidance - GOV.UK
- Prevent duty guidance: for England and Wales (accessible) - GOV.UK
- Mobile phones in schools - GOV.UK
- Generative artificial intelligence (AI) in education - GOV.UK
- Using AI in education settings: support materials - GOV.UK

Information Commissioner's Office (ICO)

- Data Protection Impact Assessment

London Grid for Learning (LGfL)

- Online Safety Audit

Southwest Grid for Learning (SWGfL)

- Online Safety Self-Review Tool for Schools

National Cyber Security Centre

- Cyber security training for school staff

Other

- UK Safer Internet Centre
- Digital Resilience

Ownership and Consultation	
Document sponsor/approver	Head of IT – Europe and United States
Document author	Head of IT – Europe and United States
Consultation with	Europe Digital Learning Advisors
	Group Cyber Security
	Europe IT POD Leads
	Regional Safeguarding Lead - Europe and United States
Audience	
Audience	Regional Employees
	Regional Students and Parents
	Suppliers
	Visitors
	Contractors
Document Application	
The policy is related to this jurisdiction	All Cognita Europe Schools and Offices
Version Control	
Review cycle	Annual
Effective from	1 September 2026
Next review date	28 May 2027
Version	1.2 ISSUED