COGNITA

Cumnor House School

Acceptable Use
&
Digital Safety Policy

September 2023

1 Introduction

1.1. The use of technology as a tool has become an integral part of school and home life.

1.2. Cognita Schools is committed to the effective and purposeful use of technology for teaching, learning and administration and is also committed to protecting its staff, students, parents and visitors, from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.

1.3. The school actively promotes the participation of parents to help the school safeguard the welfare of pupils and promote the safe use of technology.

1.4. This policy applies to the use of:

- All technology devices and equipment connected to the school network;
- All technology devices supplied by the school to employees and contractors, both onsite and offsite;
- All technology devices supplied by the school to students via our 1-to-1 device programme, both onsite and offsite;
- All applications and IT services provided by the school for teaching, learning and administration; and
- All applications and IT services available online and accessible via the school network or a school technology device.

1.5. A copy of this policy is available to staff, students, parents and visitors on request and on the school website.

1.6. In the event of a breach of this policy and its requirements, failure to have read this policy will not be accepted as a defence/excuse.

2 Purpose of this Policy

2.1 Promote responsible use and care of technology and IT services available to staff, students, parents and visitors;

2.2 Outline the acceptable and unacceptable use of technology and IT services at the school, both on and offsite;

2.3 Outline the roles and responsibilities of all staff, students, parents and visitors;

2.4 Educate and encourage pupils to make good use of the educational opportunities presented by access to technology at the school;

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

- exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);
- inappropriate contact from staff;
- inappropriate contact from strangers;
- cyber-bullying and abuse;
- copying and sharing personal data and images;
- etc.

2.6 Outline Digital Filtering and Monitoring on school devices and the school network.

2.7 Outline requirements for reporting misuse of technology.

2.8 Ensure arrangements in place for all stakeholders, SLT, DSL and IT to work closely together.

3 Scope

3.1 This policy applies to all staff, students, parents and visitors of the school.

3.2 The school 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 and software and services and applications associated with them including:

- the school network, WIFI and internet access;
- tablets, desktops, laptops, and thin client devices;
- mobile phones, smartphones, smart watches and other smart wearables;
- digital devices for audio, still images and moving images (e.g. personal music players and GoPro devices);
- digital displays and SMART boards;
- 2D and 3D printers;
- communication and collaborations applications (e.g. email and Teams);
- Virtual Learning Environments (e.g. firefly);
- mobile messaging apps (e.g. Snapchat and WhatsApp); and
- social media (e.g. Facebook, Instagram, TikTok);
- etc.

3.3 This policy applies to the use of technology on and off school premises.

3.4 This policy applies to any member of the school community where the culture or reputation of the school are put at risk.

3.5 This policy applies to any member of the school community where staff, students, parents or visitors are put at risk.

4 Related Documentation

4.1 Safeguarding and Child Protection Policy

4.2 Preventing Radicalisation and Extremism Policy

4.3 Behaviour Policy

5 Roles and Responsibilities

5.1 This policy document is the responsibility of the Cognita Regional Director of Education.

5.2 The school Head is responsible for publishing this policy and the ongoing implementation and monitoring of this policy.

5.3 The Cognita European Head of IT is responsible for ensuring that technology and IT Services are deployed and monitored in line with this policy.

5.4 The Head of Cybersecurity is responsible for the filtering and monitoring process.

5.5 The DSL is responsible for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

5.6 All staff, students, parents and visitors are responsible for adhering to the policy.

6 Safe Use of Technology

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

6.2 Use of technology should be safe, responsible, respectful to others and legal. Staff, students, parents and visitors are responsible for their actions, conduct and behaviour when using technology at all times.

6.3 The school will support the use of technology and make internet access as unrestricted, as necessary whilst balancing the educational needs of our students, the safety and welfare of staff, students, parents and visitors, and the security and integrity of our systems.

6.4 Monitoring, logging and alerting tools are in place to maintain technology safety, safeguarding and security for the protection of Staff, Students, Parents and Visitors.

6.5 The filtering and monitoring tools are reviewed annually to ensure that the current provision addresses all needs of our staff and students. This review involves IT, Cybersecurity, Governors and Proprietors.

6.6 In the interest of safeguarding children, student 1-to-1 devices have monitoring software pre-installed. The software provides live and historic data regarding the use of the device e.g. web browsing, and the data collected is stored for 90-day periods. For further information on how we looked after the personal data we collect, please see the school's Privacy Notice on their website. For more details, please refer to the Web Filtering Statement (Appendix B) that provides further details of the arrangements in place for filtering and monitoring usage within Cognita schools.

6.7 The monitoring software uses Artificial Intelligence (AI) in order to determine how new websites are filtered and which categories they sit in.

6.8 IT technicians have the power to make manual changes within the filtering system.

6.9 The Designated Safeguarding Lead is responsible for understanding the monitoring systems and processes in place. They receive training annually to understand the reporting process to analyse the filtering data. (link to Cognita's bespoke Lightspeed training portal)

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

6.11 All staff should have an understanding that the filtering system is in place to safeguard children, and the expectations and responsibilities related to it.

6.12 The school can make bespoke changes to the filtering system, and how they access IT, for those children who are potentially at greater risk of harm.

6.13 We want pupils to enjoy using technology and to become skilled users as technology has become a fundamental part of education, not only as the vehicle to deliver great teaching and learning, but as a platform for collaboration and productivity.

6.14 Pupils will be educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

6.15 The school actively encourages the participation of parents to help promote the safe use of technology with their children.

6.16 Any concern regarding unsafe or inappropriate use of technology should be reported to a teacher, school Head or Designated Safeguarding Lead as soon as possible.

6.17 Any serious incident involving unsafe or inappropriate use of technology will be reported by the school Head to the Cognita European Head of IT who will record and investigate the matter.

6.18 All users of technology may find the following resources helpful in keeping themselves safe online:

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

6.19 In addition, schools should consider meeting the Cyber security standards for schools and colleges.

6.20 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.

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

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

7 The Right to Use School Network and Equipment.

7.1 School employees and students will be allocated a username and password for accessing technology devices and services.

7.2 Some shared resources will have a generic username and password for access.

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

7.4 Only school devices should be connected to the school network and personal devices should only connect to the guest network.

7.5 Any attempt to access or use any user account or email address, for which a staff member, student, parent or visitor is not authorised, is prohibited.

7.6 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 (See Appendix A).
- Students with a designated device may use the device in lessons at the direction of their teacher.
- School employees and students are responsible for the safety and security of a designated device when taken out of school.
- School issued devices and associated peripherals should be returned in good condition (excluding ordinary wear and tear) and in working order.
- School issued devices are insured against accidental damage, loss and theft; the assignee is liable for the payment of the Cognita Insurance excess.
- Staff / Parents are responsible for the cost of a like for like replacement of an assigned device if it is damaged / lost intentionally, wilfully or through neglect.

7.7 Resource devices are available in school for use by employees and students on general work, lessons and specialist applications.

7.8 School employees and students may not use, or attempt to use, IT resources allocated to another person, except when explicitly authorised.

7.9 For security purposes users must log off or lock their computer at all times when they step away from their device. Users must log-off and shutdown their device at the end of the day.

8 Appropriate Use of Technology for Digital Safety

8.1 The school provides **System and Application Accounts** for staff, students, parents and guests when required.

- You must:
  - Not allow other people to use your account.
  - Not use someone else's account.
  - Lock your device or logout of your account when not in use.
  - Only use school applications and email for official school business and digital correspondence.
  - Not send messages or emails from school accounts that purport to come from an individual other than the person actually sending the message.

- Staff and students must:
  - Use official school accounts on approved collaborative platforms

8.2 The school provides technology **Hardware and Software** to support education and the running of the school business.

- Users of school technology equipment are expected to take care of the equipment through responsible behaviour.
- School technology should 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 School Leadership Team.

- School technology assigned to staff and students is the responsibility of the assignee.
- You should not leave portable technology equipment, including school-issued devices unattended.
- Loss or damage of school technology should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity.
- Theft of school technology assigned to an individual member of staff or to a student via the 1-to-1 programme should be reported to the police and be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity along with a crime reference.
- Deliberate abuse or damage of school equipment will result in the culprit(s) being billed for the full replacement costs of the equipment.
- Do not:
  - Attempt to install software onto a school-owned or school-issued device other than when directed to via the school Application Download Store.
  - Download or access illegal software 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-owned or school-issued device.
  - Attempt to alter the configuration of the hardware equipment or any accompanying software unless under the written instruction of the school.

8.3 The school provides technology resources for accessing and storing **Data**.

- Do not:
  - Access or attempt to access data for which you are not authorised.
  - Interfere with digital work belonging to other users.
  - Share private, sensitive or confidential information unless:
    - You have authority to share
    - The method of sharing is secure
- 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.

8.4 The school endeavours to safeguard and where possible mitigate all **Security** risks associated with technology.

- The school has filtering systems in place to block access to unsuitable material, wherever possible and to protect the welfare and safety of staff, students, parents and guests.
- You must not:
  - Try to bypass school filtering systems whilst using school devices or using the school network.
  - Use software or network routing designed to bypass filters and access blocked sites.
  - Try to bypass technology security systems whilst using school devices or using the school network.
  - Use software or network routing designed to bypass school technology security systems.

- Access to unsuitable material on a school device or on the school network should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity.
- The school has technology security systems in place to block and to protect against computer viruses or other malicious software such as spyware (See Appendix B).
- Concerns regarding viruses and other malicious software should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity.

8.5 It is the responsibility of all technology users to ensure the **Welfare** of themselves and others both on personal and school devices.

- Cyberbullying - Pupils must not use their own or the school's technology to bully others.
- Strangers - Pupils must not use their own or the school's technology to make contact or engage with people who they do not know.
- Sexting - Pupils must not use their own or the school's technology to create or share sexualised content including images, audio, video and text.
- Concerns regarding a child's safety or welfare associated with use of technology must be reported to the Designated Safeguarding Lead at the earliest opportunity.
  Staff must not ever 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 and Head immediately.

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

- The internet provides technology users with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisations and groups world-wide so as to increase skills, knowledge and abilities.
- 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.
- Staff, students, parents and visitors must not use a school device or the school network to intentionally visit internet sites that contain obscene, illegal, hateful, abusive, offensive, pornographic, extremist or otherwise inappropriate materials.
- Staff, students, parents and visitors must not use a school device or the school network to access gambling websites.
- Staff, students, parents and visitors shall be responsible for notifying a member of the School Leadership Team, Designated Safeguarding Lead or IT Support Team of any inappropriate material accessed on a school device or on the school network so that access can be blocked.
- Privacy of staff, students, parents and visitors must always be recognised and respected on social media sites.
- Staff must not connect with any pupil, current or past, under the age of nineteen on any social networking site or via work/personal mobile phones.
- Staff, students, parents and visitors of the school must not make offensive or inappropriate comments including bringing the school's name and reputation into

disrepute 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.

9 Cognita Allocated Devices: Access & Privacy

9.1 Access to assigned devices and IT content:

- School technology devices assigned to staff and students are for the sole use of the assignee.
- Student devices may be loaded with a Classroom Management Application which enables appropriate functionality for the teach to control and view the students screen during the lesson period.
- Cognita devices may be loaded with Remote Support Applications which enables IT support staff to logon to the devices to provide remote assistance; this may only be used with the permission of the device assignee.
- 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.
  - To enable system security protection (e.g. Virus, Malware, Hacking or other Risk).
  - To investigate potential misuse, abuse and/or illegal activity.
  - To monitor compliance with employment and statutory obligations.
  - To guarantee the integrity of the school devices, technology and IT systems.
- To access an assigned device written permission must be given as follows:
  - Cognita HR Director or Partner for a device assigned to a member of staff.
  - The School Head or the School DSL for a device assigned to a student.
- Data on a Cognita Device or accessed through a Cognita Device is aligned with Cognita & School Privacy Policies.

10 Photographs and Images

10.1 The school abides by data protection legislation, namely, the General Data Protection Regulation 2018 (as amended, extended or re-enacted from time to time), and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw this permission at any time by informing the school's Administration Team in writing.

10.2 The Cognita Code of Conduct for Staff states, 'Cognita does not permit the use of personal mobile phones, smart watches and cameras by staff where children are present'.

10.3 The Early Years Safeguarding and Welfare Requirements requires all schools to have a clear policy on the use of mobile phones and devices.

10.4 Staff, students, parents and visitors are not permitted to use devices such as mobile phones, cameras, smart watches or digital recorders to photograph or record members of staff or pupils without their permission. Safe and appropriate use of recording equipment must be discussed with the pupils as part of the curriculum and referred to whenever recording is to take place. Permission may be granted by the school in the event of performances/events organised by the school.

10.5 Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission. Any parent 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.

11 Use the School equipment for personal use

11.1 School devices and IT systems are provided for schoolwork only; should you decide to use the equipment or IT systems for personal use, please be informed that it will be at your sole risk and could be considered as a breach of the Digital Safety Policy. Furthermore, please be informed that as per Section 9 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.

11.2 Only approved software and applications may be installed on a school device.

11.3 School devices and network must not be used to carrying out any illegal trading activity.

11.4 Conducting any private or financial transaction on shared equipment carries a risk and your personal data may not be safe.

12 Use of personal equipment in School

12.1 Personal devices must not be connected to the school network other than to the guest Wi-Fi network.

13 Procedures for Reporting

13.1 Staff, students, parents and visitors of the school with a concern or an incident regarding technology should take the following actions:

- Stop the problem or remove the technology (unless to do so would jeopardise any internal investigation or that form an external agency e.g. the Police).
- Prevent exposure of the incident to others.
- Record the nature of the incident and those involved using appropriate forms.
- Preserve evidence to enable investigation if required.
- Report the incident or concern to a teacher, school Head, Designated Safeguarding Lead or IT Support Team as appropriate.
- Staff must not carry out any investigations until they are authorised to do so.
- Complete a Serious Incident Report Form as directed by the head of health and Safety/Regional Safeguarding Lead.

13.2 Any concern regarding unsafe or inappropriate use of technology, or welfare associated with use of technology, must be reported to a teacher, school Head or Designated Safeguarding Lead as soon as possible.

13.3 Staff are aware that they should make a report when:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software 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
- etc.

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

13.5 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; theft should also be reported to the police and a crime reference obtained.

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

13.7 The school has a duty to report serious concerns to Local Authority Safeguarding Teams or to the Police, in line with statutory requirements.

14 Removal of Network Rights/Sanctions

14.1 Anyone found abusing the Digital Safety Policy on the use of computers may have their network rights removed and may be subject to further disciplinary action.

14.2 The school reserves the right to remove network access at any time.

14.3 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.

14.4 The school takes its responsibilities in relation to digital safety and use of technology by staff, students, parents and visitors seriously and understands the importance of monitoring, evaluating and reviewing its policies and procedures regularly.

Appendix A: Student 1-to1 iPad/Laptop Consent Form

STUDENT 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 classmates in a purposeful way that supports your learning journey. We've listed some simple guidelines below, have a read and make a firm commitment to look after it 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. There is no need to install anything else or change any of the settings.

BE RESPONSIBLE

- Keep your iPad/laptop safe when you are on the move, use the protective sleeve provided.
- Lock your iPad/laptop away when it’s not with you.
- Handle your iPad/laptop with care keeping it away from food and liquids.
- Report any damage or problems to your Form Teacher.

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

Name:

Date:

Appendix B: Web Filtering Statement - Sep 2023

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 and Bing 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 Smoothwall Firewalls. Specific web filtering policies are applied to different groups per school (e.g. Staff, 6th form, Key Stages1-4). Smoothwall analyses 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 Lightspeed web filtering agent installed using advanced AI to automatically block millions of inappropriate and harmful sites, images, and videos.

Both Smoothwall and Lightspeed record activities for analysis, investigation and reporting. Analysis of traffic and internet usage is assessed periodically to update filtering rules.

Link to Lightspeed (2021) Monitoring Provider Checklist Reponses which highlights to what extend our filtering tool blocks harmful and inappropriate content, without unreasonably impacting teaching and learning

School DSLs and Heads are responsible for using the information provided to take appropriate action. Members of the Cognita central team are available to support with issues that require escalation.

Key contacts:

- Head of Cyber Security, Cognita
- Regional Safeguarding Lead, Europe and USA
- Chief Operating Officer, Europe and USA

Appendix C: Filtering and Monitoring Useful links and resources

Department for Education

Keeping Children Safe In Education (DfE)

Meeting digital and technology standards in schools and colleges (DfE)

Broadband internet standards for schools and colleges (DfE)

Cyber security standards for schools and colleges (DfE)

Data protection policies and procedures (DfE)

Home Office

The Prevent duty: safeguarding learners vulnerable to radicalisation (Home Office)

Information Commissioner's Office

Data Protection Impact Assessment (DPIA) (ICO)

London Grid for Learning (LGfL) Online

Safety Audit (LGfL)

South West Grid for Learning (SWGfL)

Online Safety Review (360Safe) (SWGfL)

National Cyber Security Centre

Cyber security training for school staff

UK Safer Internet Centre

2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)

Test Your Internet Filter (UKSIC / SWGfL)

Filtering provider responses - self-certified by service providers (UKSIC)

A Guide for education settings and filtering providers (UKCIS)

Establishing appropriate levels of filtering (UKSIC)

Online safety in schools and colleges: questions from the governing board (UKCIS)

Digital Resilience

HeadStart Online Digital Resilience Tool (HeadStart Kernow)

Version control:

Ownership and consultation	
Document Sponsor	Cognita Regional Director of Education
Document Author / Reviewer	COO Europe and USA Reviewed by Head of Digital Learning June 2023 Reviewed by Regional Safeguarding Lead- June 2023 Reviewed by Head of Cyber security- June 2023
Consultation & Specialist Advice	
Document application and publication	
England	Yes
Wales	Yes
Spain	Yes
Switzerland	Yes
Italy	
Version control	
Current Review Date	September 2023
Next Review Date	September 2024
Related documentation	
Related documentation	Safeguarding and Child Protection Policy Preventing Radicalisation and Extremism Policy Behaviour Policy