COGNITA

Cumnor House School

Digital Safety Policy

Including E-Safety, Digital Safety Agreement and Bring Your Own Device (BYOD) Guidance

September 2019

5 & 7 Diamond Court, Opal Drive, Eastlake Park, Fox Milne, Milton Keynes MK15 0DU, T: 01908 396250, F: 01908 396251, www.cognita.com
Registered in England Cognita Limited No 5280910 Registered Office: Seebeck House, One Seebeck Place, Knowlhill, Milton Keynes MK5 8FR

Contents

1 Introduction

1.1 This Digital Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard adults and pupils. It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable use or misuse of these technologies by adults or pupils.

1.2 The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks with using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils use these technologies. These risks include:

- Being vulnerable to inappropriate contact from strangers;
- Cyber-bullying;
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices;
- Issues with spam and other inappropriate email;
- Online content which is abusive, offensive, or pornographic;
- The use of social media to encourage extremism; and
- Viruses.

1.3 It is also important that staff are clear about the procedures, for example only contacting pupils about homework via a school email address or the school's Virtual Learning Environment (VLE), such as Firefly, not via personal emails.

1.4 Whilst we endeavour to safeguard and mitigate against all risks, we will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly and according to the school's policies to ensure the school continues to protect pupils.

1.5 It is the duty of the school to ensure that pupils, teachers, administrative staff and visitors are protected from potential harm whilst they are on school premises.

1.6 The involvement of pupils and parents is also vital to the successful use of digital technologies. This policy thus also aims to inform how parents and pupils are part of the procedures and how pupils are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

2 Aims of this Policy

- To ensure the safeguarding of all pupils within the school by detailing appropriate and acceptable use of all online and digital technologies.
- To outline the roles and responsibilities of all pupils, staff and parents.
- To ensure all pupils, staff and parents are clear about procedures for misuse of any online technologies.
- To develop links with parents and the wider community to ensure continued awareness of online technologies.

3 Pupils

3.1 Our pupils:

- Are involved in the review of our Digital Safety Agreement through discussion in lessons and other forums, in an age appropriate way;

- Are responsible for following the Digital Safety Agreement whilst within school as agreed each academic year or whenever a new pupil starts at the school for the first time, and are required to sign that they have read and understood the rules;
- Are taught to use the internet in a safe and responsible manner through, for example, ICT and PSHE lessons;
- Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know;
- Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;
- Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites;
- Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free;
- Are taught to understand what is meant by e-safety through age appropriate delivery;
- Are taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the;
- Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk;
- Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this policy; and
- Must connect to the internet whilst on premises owned or rented by Cognita using the pupil wireless network, and must not circumvent internet access by using a personal device's cellular data services.

4 Inappropriate Use by Pupils

4.1 Should a pupil be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a pupil accidentally accesses inappropriate materials, the pupil is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window. Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour Policy

4.2 Refer to Annex 1 for further guidance.

5 Staff

5.1 It is the responsibility of all adults within the school to:

- Adhere to the Staff Code of Conduct including Acceptable Use Policy;
- Implement the pupil Digital Safety Agreement (see Annex 2, 3 and 4);
- Be up to date with digital knowledge appropriate for different age groups;
- Be vigilant when using technology as part of lessons;
- Model safe and responsible use of technology;
- Provide reminders and guidance to pupils on Digital Safety;
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner;
- Not leave a computer or other device unattended whilst they are logged on;
- Lock away or safely secure all portable ICT equipment when not in use;
- Not connect with any pupil under the age of nineteen on any social networking site, or via personal mobile phones and follow the school's Social Guidelines. See the Social Media Policy for further detail;

- Protect confidentiality and not disclose information from the network, or pass on security passwords;
- Make sure that any information subject to data protection legislation, namely, the General Data Protection Regulation 2016 (as amended, extended or re-enacted from time to time), is not stored on unencrypted portable media or transported in an unsecure form;
- Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute;
- Follow the school's 'dos' and 'don'ts' in our Email Best Practice Guide – see Annex 7;
- Not make or take personal calls or engage in personal texting when they are on duty;
- Report any concerns about a pupil related to safeguarding and e-safety to the Designated Safeguarding Lead;
- Report accidental access to inappropriate materials to the DSL, Emma Edwards so that inappropriate sites are added to the restricted list; and
- Only use school owned devices and memory cards to take photographs or videos.

6 Inappropriate Use by Staff

6.1 If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a report must be made to the Head, along with the DSL immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

6.2 Refer to Annex 1 for further guidance.

7 Parents and Visitors

7.1 All parents have access to a copy of this Digital Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

7.2 As part of the approach to developing e-safety awareness with pupils, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites. The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

7.3 Parents should be aware that the school cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils, and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

8 Wi-Fi Access

8.1 Parents and visitors to the school are expected to abide by this policy. Should visitors wish to access the internet via the school's Wi-Fi, they will be issued with a password. Access is only permitted once they have agreed to the school's terms and conditions.

9 Video and Photography at School Events

9.1 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. 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.

10 Early Years Use of Mobile Phones or Device - Statutory Regulation

10.1 The Early Years Safeguarding and Welfare Requirements (para 3.4) requires all schools to have a clear policy on the use of mobile phones and devices.

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

11 Bring Your Own Device (BYOD)

11.1 The school does not allow pupils to bring their own devices to school.

12 The School's Responsibilities

12.1 The school takes its responsibilities in relation to the acceptable use of technology by pupils and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

13 Filtering and Safeguarding Measures

13.1 The school's internet has a robust filtering system which is set at an age appropriate level such that inappropriate content is filtered. The system logs all attempts to access the internet, including all attempts to access inappropriate content.

13.2 Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a regular basis. Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users. Strong encryption is used on the wireless network to provide good security.

14 Email Use

14.1 The school provides school email addresses for pupils (Year 3 - 8) to promote safe and efficient communication in the school. Pupil email accounts are provided by the Head of IT, Theo Turner.

14.2 All staff are expected to use email professionally and responsibly. See Annex 7 for further details.

15 The School's Use of Images and Videos

15.1 The school abides by data protection legislation, namely, the General Data Protection Regulation 2016 (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 their permission at any time by informing the administration team in writing.

15.2 Staff are not permitted to use their own devices or memory cards to record videos or photographs of pupils, and when storing images within the school's network are requested to only use the pupil's first name.

16 The Curriculum and Tools for Learning

16.1 The school teaches our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSHEE lessons. The following concepts, skills and competencies are taught through the school in an age appropriate manner:

- Digital citizenship;
- Future work skills;
- Internet literacy;

- Making good judgments about websites and emails received;
- Knowledge of risks such as viruses, and opening mail from a stranger;
- Access to resources that outline how to be safe and responsible when using any online technologies;
- Knowledge of copyright and plagiarism issues;
- File-sharing and downloading illegal content;
- Uploading information – knowing what is safe to upload, and not to upload personal information; and
- Where to go for advice and how to report abuse.

16.2 These skills are taught explicitly within the ICT curriculum but are likely to be covered in other subjects; pupils are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner. Further details about the content of the curriculum related to ICT can be found in the ICT and PSHEE curriculum documentation.

17 Monitoring

17.1 It is the responsibility of the school to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. The school will monitor the use of online technologies and the use of the internet by pupils and staff. The Designated Safeguarding Lead, Head of IT and lead pastoral staff will conduct regular audits with pupils to assess their knowledge and understanding of issues related to e-safety and act on any areas of vulnerability.

17.2 To audit digital safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of e-safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all pupils demonstrate an awareness of e-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is e-safety observed in teaching and present in curriculum planning documents?

18 Social Media

18.1 For advice relating to the use of social media, please refer to the Social Media Policy.

Annex 1: Procedures for staff in the event of a breach of this policy by a pupil or adult

(A) An inappropriate website is accessed inadvertently:

- Report to the DSL, Emma Edwards; and
- Contact ICT Support via email so that it can be added to the banned or restricted list.

(B) An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material, by shutting down the computer;
- Record the incident in writing;
- Report to the Head and DSL immediately; and
- The Head applies the Behaviour Policy.

(C) An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity;
- Alert the DSL immediately; and
- Ensure the device is shut down and record the nature of the material.

(D) An adult has used ICT equipment inappropriately:

- Follow the procedures for (B).

(E) An adult has communicated with a pupil, or used ICT equipment, inappropriately:

- Ensure the pupil is reassured;
- Report to the Head who should follow the Staff Code of Conduct and Safeguarding Policy (if relevant);
- Preserve the information received by the pupil if possible, and determine whether the information received is abusive, threatening or innocent; and
- If illegal or inappropriate use is established, contact the Head (or the DE (Cognita Director of Education), if the allegation is made against the Head) and the Designated Safeguarding Lead immediately, and follow the Safeguarding Policy.

(F) Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school:

- Preserve any evidence; and
- Inform the Head immediately and follow the Safeguarding Policy as necessary.

(G) Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere:

- The Head should be informed.

Annex 2 – Digital Safety Agreement for Pupils in Early Years, Year 1 and Year 2

Early Years, Year 1 and Year 2: Digital Safety Agreement

These are our rules for using the internet safely at school:

- We use the internet safely to help us learn.
- We learn how to use the internet.
- If we see anything on the internet or receive a message that is unpleasant, we must tell an adult.
- We learn to keep our password a secret.
- We know who and when to ask for help.
- If we see something on a computer that we do not like or makes us feel uncomfortable we know what to do.
- We know that it is important to follow the rules.
- We aim to look after each other by using the internet safely.

Annex 3 – Digital Safety Agreement for Pupils in Years 3 – 6

Year 3, 4, 5 and 6: Digital Safety Agreement

These are our rules for using the internet safely and responsibly at school:

- We use the internet to help us learn, and we will learn how to use the internet safely and responsibly.
- We send emails and messages that are polite.
- Approval from an adult may be needed before we email, chat to, or video-conference anyone at school.
- We never give out passwords or personal information (like our last name, address or phone number).
- We never post photographs or video clips without a teacher's permission and never include names with photographs.
- If we need help we know who and when to ask.
- If we see anything on the internet or in an email or other electronic message that makes us uncomfortable or appears unpleasant, we inform an adult.
- I accept that the school monitors my use of the internet at school and my school email account.
- If we receive a message sent by someone we do not know, we inform an adult.
- We aim to look after each other by using our safe internet in a responsible way.
- We agree not to send hurtful words, images or messages outside of school on the internet or mobile devices about anyone in our school community.

Name: _____ Year group:_____

I understand the Digital Safety Agreement for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature: _____ Date: _____

Annex 4 – Digital Safety Agreement for Pupils in Years 7 – 13

Year 7 – 13: Digital Safety Agreement

I am encouraged to use and be aware of the safety rules and procedures which regulate my use of the ICT resources, including the internet. Access to the school's network and the internet enables me to find resources, to communicate, and to help my research for the completion of school work.

I accept that these facilities are to be used for educational purposes only and in an appropriate manner. I take responsibility for my actions and know that any breach of the rules will be considered a serious disciplinary matter.

- I will make targeted use of the internet to support my studies.
- I accept that the school monitors my use of the internet at school and my school email account.
- If I bring a personal device to school, including a mobile phone, I agree to log on to the
- internet via the school's Wi-Fi.
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to anyone.
- I will follow fully our teachers' instructions over the use of IT and the internet.
- I do not assume that information published on the Web or written in an email is accurate.
- I keep my username and password confidential.
- I am careful about what I write on a computer. I check my work before I print or send it.
- I do not use bad language. I do not write racist, sexist, abusive, homophobic or aggressive words. I do not write things that could upset or offend others.
- I understand that sending malicious messages outside of school can become a matter whereby the school will set sanctions or involve outside agencies such as the police.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I do not make available online personal information about myself or anyone else, such as an address, telephone number and private details, in an email or on a website.
- I do not respond to offensive, abusive or rude messages. I let a teacher know immediately if I am sent anything I do not feel comfortable with.
- At school I do not go to sites or download any materials which are in bad taste, offensive, violent or pornographic.
- If I quote from a text I will always attribute my sources and acknowledge use of anyone else's ideas, images or data by citing the author, using quotation marks, and compiling a bibliography as required.
- I always respect the privacy of other users' data.
- I will report to a teacher any incident that breaches the Digital Safety Agreement, even if that incident does not affect me.
- I will treat school IT equipment with respect and will report any damages to a teacher.
- If I deliberately damage a piece of school equipment I will be charged for its replacement.
- I will not bring the school's name into disrepute when using the school's IT equipment or school email.
- I will check my school emails regularly to enable me to work and learn effectively.
- I will follow the school rules on academic honesty and not practice plagiarism.
- I know that if I am worried about something related to technology outside of school I can ask for advice or help from my teachers.

Name: _____ Year group: _____

I understand the contents of the school's Digital Safety Agreement and the rules for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Pupil signature: _____ Date: _____

Annex 7 – Email Etiquette

Email best practice

- Write well-structured emails and use short, descriptive subjects.
- Sentences can be short and to the point. You can start your email with ‘Hi’, or ‘Dear’, and the name of the person. The use of internet abbreviations and characters such as smileys is not encouraged.
- Signatures must include your name, job title and school name. A disclaimer should be added underneath your signature.
- Users must spell check all mails prior to transmission.
- Only mark emails as important if they really are important.
- Avoid long strings of messages; start new conversations.

Do not

- Write it in an email unless you would put it on a noticeboard in the office or in a newspaper.
- Write anything that is libellous, defamatory, offensive, racist or obscene - you and the school can be held liable.
- Forward confidential information - you and the school can be held liable.
- Forward a message with sensitive information without acquiring permission from the sender first.
- Send email messages using another person’s email account.

Ownership and consultation	
Document sponsor (role)	Group Director of Education
Document author (name)	James Carroll, ADE
Consultation – May 2017	The following schools were consulted: Colchester High School, Cumnor Girls' School, El Limonar Villamartin, North Bridge House Nursery and Pre-Prep School, Oxford House School, Southbank International School Kensington and Hampstead Campus, St Clare's School and St Nicholas Prep School. Education Team representative – Karen Nicholson, ADE.
Updated – May 2018	Andy Perryer, Digital Learning Adviser

Audience	
Audience	All school staff

Document application and publication	
England	Yes
Wales	Yes
Spain	Yes

Version control	
Implementation date	September 2019
Review date	Review and update for implementation in September 2020

Related documentation	
Related documentation	Safeguarding and Child Protection Policy Preventing Radicalisation and Extremism Policy Behaviour Policy