COGNITA
TEACHING EXCELLENCE

Digital Safety Policy

Including E-Safety, Digital Safety Agreement, Bring Your Own Device, Social Media Guidance

September 2017

DOWNSEND
PRE-PREP SCHOOL
Leatherhead

Contents

1.0 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.

2.0 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.

3.0 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 student starts at the school for the first time, and 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 PSHEE 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 police;
- 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 Digital Safety Policy; and
- Must connect to the internet whilst on premises owned or rented by Cognita using the student wireless network, and must not circumvent internet access by using a personal device's cellular data services.

4.0 Inappropriate use by pupils

4.1 Should a student be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a student accidentally accesses inappropriate materials, the student 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 student 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 Policies.

4.2 Refer to Annex 1 for further guidance.

5.0 Staff

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

- Adhere to the Staff Code of Conduct including Acceptable Use;
- Implement the student 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 student under the age of nineteen on any social networking site, or via personal mobile phones and follow the school's Social Guidelines. See Annex 7 and 8 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 is not stored on unencrypted portable media or transported in an insecure 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 9;
- Not make or take personal calls or engage in personal texting when they are on duty;
- Report any concerns about a student related to safeguarding and e-safety to the Designated Safeguarding Lead;
- Report accidental access to inappropriate materials to Gill Brooks so that inappropriate sites are added to the restricted list; and
- Only use school owned devices and memory cards to take photographs or videos.

6.0 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.

7.0 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 student'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.

8.0 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.

9.0 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 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. Note: SCHOOLS TO CHECK OTHER WORDING INCL PARENT CONTRACT

10.0 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'.

11.0 Bring Your Own Device (BYOD)

11.1 Clear procedures are in place for managing BYOD, including the requirement for signed agreements from parents and pupils. See Annex 5 and 6 for further details.

12.0 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.

13.0 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.

14.2 All staff are expected to use email professionally and responsibly. See Annex 9 for further details.

15.0 The school's use of images and videos

15.1 The school abides by the Data Protection Act 1998 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 at a specific campus.

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 student's first name.

16.0 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.

17.0 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 Leader 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?

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

(A) An inappropriate website is accessed inadvertently:

- Report to Gill Brooks; 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 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 Head 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 student, or used ICT equipment, inappropriately:

- Ensure the student 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 student 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 ADE (Cognita Assistant 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 7 - Social Media Guidance

Social media is a broad term for any kind of online platform which enables people to directly interact with each other.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and pupils.

Scope

This guidance is subject to Cognita's Staff Code of Conduct including Acceptable Use Agreements.
This policy:

- Applies to all staff and to all online communications which directly or indirectly represent the school;
- Applies to such online communications posted at any time and from anywhere;
- Encourages the safe and responsible use of social media through training and education; and
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this guidance.

Personal communications which do not refer to or impact upon the school are outside the scope of this guidance.

Digital communications with staff/pupils are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes, but must consider whether this is appropriate and consider the potential implications.

Process for creating new accounts and monitoring use

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "friends of the school" Facebook page. Anyone wishing to create such an account must present a case to the Headteacher which covers the following points:

- The aim of the account;
- The intended audience;
- How the account will be promoted;
- Who will run the account; and
- Will the account be open or private/closed.

Following consideration, an application will be approved or rejected. In all cases, the Headteacher must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

School accounts must be monitored regularly and frequently to ensure appropriate use.

Annex 8 – Social Media Do's and Don'ts

Managing your personal use of social media

- 'Nothing' on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online, consider: scale, audience and permanency.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

The Do's:

- Check with a senior leader before publishing content that may have controversial implications for the school;
- Use a disclaimer when expressing personal views;
- Make it clear who is posting content;
- Use an appropriate and professional tone;
- Be respectful to all parties;
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author;
- Express opinions but do so in a balanced and measured manner;
- Think before responding to comments and, when in doubt, get a second opinion;
- Seek advice and report any mistakes using the school's reporting process; and
- Consider turning off tagging people in images where possible.

The Don'ts:

- Don't make comments, post content or link to materials that will bring the school into disrepute;
- Don't publish confidential or commercially sensitive material;
- Don't breach copyright, data protection or other relevant legislation;
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content;
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content; and
- Don't use social media to air internal grievances.

Annex 9 – 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)	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.

Audience	
Audience	All school staff

Document application	
England	Yes
Wales	Yes
Spain	Yes

Version control	
Implementation date	01.09.2017
Review date	Review and update for implementation in September 2018

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