Kitebrook
PREPARATORY SCHOOL

Policy 2.16

Kitebrook Preparatory School E-Safety Policy

(Including boarding, day and EYFS pupils)

Updated:	30.08.23
Author:	BRS
Next Review date:	01.09.24

1. Aims of the Kitebrook school with regard to e-safety:

1.1 Kitebrook recognises the importance of a whole school approach instilling a rigorous e-safety policy. It understands that its procedures are essential to safeguarding children online.

1.2 Issues that arise are referred in the first instance to the Safeguarding Officer (DSL) and then to the Prep Schools Trust as appropriate and, when necessary, to bodies outside the school such as the Oxfordshire Safeguarding Childrens' Board (OSCB).

2. Responsibilities

2.1 Our e-safety coordinators are the Director of IT and the Designated Safeguarding Lead

2.2 Responsibilities: Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident and provides training and advice for staff
- liaises with PST IT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments immediately

2.3 Our e-safety coordinator is the person responsible to the Trustees for the day to day issues relating to e-safety. The e-safety coordinator.

2.4 Responsibilities: Head:

- the Head is responsible for ensuring the safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety is delegated to the e-safety coordinator

2.5 Responsibilities: Teaching and Support Staff:

- all staff safeguard the welfare of children and refer any child protection concerns using the proper channels
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix A)
- they report any suspected misuse or problem to the e-safety coordinator
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme. SMART is also actively promoted during Computing Lessons and when children are using Chromebooks

2.6 Responsibilities: IT Technician/Director:

- the school's IT infrastructure and data are secure and not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy as outlined in this policy

3. Acceptable Use Agreements

3.1 All members of the school community are responsible for using the school IT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems. Acceptable Use Agreements are provided in Appendix A.

3.2 The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (**in or out of school**).

3.3 Users shall not visit Internet sites, make, email, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1999)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

3.4 Additionally the following activities are also considered unacceptable on IT equipment or infrastructure provided by the school:

- using school systems to undertake transactions pertaining to a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Gloucestershire/Oxfordshire County Council Broadband and/or the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- online gambling and non educational gaming
- personal Online shopping/commerce
- use of social networking sites (other than in the school’s learning platform or sites otherwise permitted by the school)

4. Email

4.1 It is important that staff are aware of the risks of email:

- sending or forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks

- unlawfully forwarding confidential information, the staff member and the Prep Schools Trust can be held liable
- unlawfully forwarding or copying messages without permission, the staff member and the Prep Schools Trust can be held liable for copyright infringement
- sending an attachment that contains a virus, the staff member and the Prep Schools Trust can be held liable

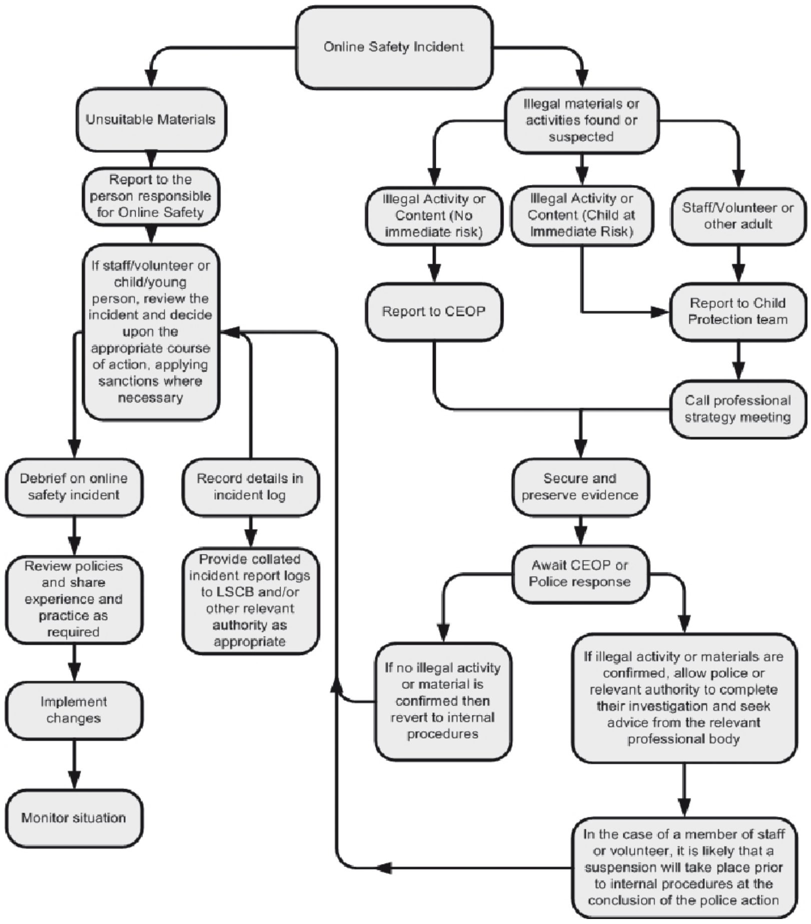
4.2 **Personal Email.** Although the Prep Schools Trust ’s email system is meant for business use, Kitebrook allows limited personal usage if it is reasonable and does not interfere with work. However the sending of chain letters, junk mail, jokes and executables is prohibited. All messages distributed via Kitebrook’s email system are company property.

4.3 **Requirements.** The following rules are to be strictly adhered to. It is **prohibited** to:

- send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If staff receive an email of this nature, staff must promptly notify the Head
- forward a message with sensitive information without acquiring permission from the sender first.
- send unsolicited email messages
- forge or attempt to forge email messages
- disguise or attempt to disguise your identity when sending mail
- send email messages using another person’s email account
- copy a message or attachment belonging to another user without permission of the originator.

5. Procedures for reporting an incident online

5.1


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

6. Best practices

6.1 When using emails, adhere to the following guidelines:

- write well-structured emails and use short, descriptive subjects
- Kitebrook's email style is informal. This means that sentences can be short and to the point. You should start your email to parents with 'Dear', and to other staff members with the name of the person or 'Hello', 'Hi', or 'Good Morning'
- signatures must include staff name, job title, and the school logo, address and contact details
- users must spell check all mails prior to transmission
- do not send unnecessary attachments
- do not write emails in capitals
- only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication
- do not click on any links or open any attachments of unsolicited or suspicious looking emails. These messages could infect your computer with a virus
- if you receive an email from a bank or any other institution, asking you to click on a link and update your details, DO NOT CLICK on the link and notify the Head
- take care when sharing and email thread - as this can be forwarded on
- Try not to use pupil names in emails where possible

7. Confidential information

7.1 Do not send credit card details, social security numbers, or other confidential information via email. If you need to send confidential information, check with the Head for safe methods.

8. Passwords

8.1 It is recommended that staff change their password regularly, using a combination of words, numbers and special characters. Staff should avoid using predictable words.

9. Email Accounts

9.1 All email accounts maintained on our email systems are property of the Prep Schools Trust. Passwords should not be given to other people and should be changed regularly. Email accounts will be deactivated or deleted when you leave school.

10. System Monitoring

10.1 Users expressly waive any right of privacy in anything they create, store, send or receive on Kitebrook's computer system. The Prep Schools Trust can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the Prep Schools Trust reserves the right to take disciplinary action.

11. Use of digital and video images

11.1 Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; **the personal equipment of staff should not be used for such purposes** unless express permission has been given by the Head.

12. Website (and other public facing communications)

12.1 Our school uses the public facing website https://www.kitebrookpst.org/ only for sharing information with the community beyond our school.

- personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils)
- only **pupil's first names and first letter of their surname** will be used on the website, and only then when necessary
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ **pupils' full names** will not be used anywhere on a website or blog, and never in association with photographs without appropriate password protection
    - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

8. E-Safety Education

8.1 Please refer also to the School's Safeguarding, Behaviour, Anti-bullying, PSHEE, and Curriculum policies, and for further information regarding incidents of cyber bullying. These will be provided by following a planned e-safety programme provided as part of Computing, PHSEE, Global Citizenship and other lessons.

9. Mobile Technology and Devices

9.1 Children are not permitted to use personal mobile devices during school time, therefore they should not be brought into school. In the event that a device is brought into school, it will remain with the class/form tutor before being returned directly to the parent at the end of the day. Mobile devices used as part of Computing are supervised by members of staff at all times and protected by the school internet filters.

9.2 Staff are not permitted to use mobile devices, or take images of children within the classroom or any areas where pupils are present, without the express permission of the Head and only then for marketing purposes. Leadership may carry mobiles on them but must ensure they are silent and not in sight of pupils. All staff wishing to use their mobile phone may do so in the staffroom or other designated area, such as an office space.

10. Staff Training

10.1 Staff and non-teaching staff receive e-safety training and understand their responsibilities, as outlined in this policy. This includes the use of Social Networks, Chat Rooms and Game sites. The school incorporates CEOP and NSPCC guidance, which both provide up-to-date policies and presentations available for all staff.

11. Parent and Carer Awareness Raising

11.1 **The school will provide information and awareness to parents and carers through:**

- *letters, newsletters, website*
- *parents' evenings and specific e-safety workshops.*

11.2 Reference can also be made to the GDPR policy with regard to data storage.

Appendix A

Acceptable Use Agreement – staff

For my professional and personal safety:

- I understand that the school will monitor my use of the Computing systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school Computing systems (e.g. laptops, email, learning platform) out of school
- I understand that the school Computing systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person
- I understand that taking photographs of children on my personal mobile phone is not allowed, unless previously agreed with the Head for marketing purposes only
- I understand that if I wish to use my personal mobile phone, I may do so in the staffroom area

I will be professional in my communications and actions when using school Computing systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images (unless I leave all images with the school or use a school data card)
- where images are published (e.g. on the school website/learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with pupils and parents/carers, in relation to school business, using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile Computing devices as agreed in the e-safety policy and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will ensure that my data is regularly backed up in accordance with relevant school policies
- I will not try to upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or

may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others. Where personal data is transferred outside the secure school network, it must be encrypted
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, suspension, or a referral to Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police