Keeping Children Safe Online

at Bernards Heath Infant and Nursery School

Date Reviewed	January 2024
Next Review Due	January 2025
Reviewed by	Hannah Rimmer

Bernards Heath Infant and Nursery school recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely.

Curriculum

Through our computing and Growing up at Bernards Heath Curriculums we keep in mind the four Cs as outlined in Keeping Children Safe in Education 2023. As well as discretely teaching children how to be safe online when learning and playing staff take the opportunity to regularly remind children of our online safety rules (attached to this policy.)

The Four Cs
Content Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.
Conduct Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.
Commerce Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. We also consider how the risk from commerce applies to staff.

For more information about the computing curriculum and online safety curriculum follow the link to the curriculum page on our website where you can view our progression documents, long term planning and Growing Up at Bernards Heath curriculum.

Email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact children, parents or conduct any school business using a personal email address. Children will use school approved email for educational purposes. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. They could also be subject to disclosure under a Subject Access Request

under the GDPR. With this in mind staff and governors should be mindful of what is contained within email/WhatsApp or Governor Hub and should maintain good housekeeping – not keeping emails unnecessarily.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report the receipt of these to the Head Teacher or Business Manager.

Staff and Governors must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying), harassing, libellous, contain confidential or private information which the recipient is not authorised to receive. If private and/or confidential information is being shared this should be password protected.

Filtering and Monitoring

Our Safeguarding Governor, works with the Head Teacher, Business Manager and Network manager on an Online Safety Group. The purpose of this group is to ensure that we are doing all that we reasonably can to limit children's exposure to risks. As part of this process, we have appropriate filtering and monitoring systems in place and review their effectiveness at least annually. We know how to escalate concerns when identified to our Network Manager and HICS as appropriate. The age of our children (3-7 years) means that within school they are only learning online under direct adult supervision.

The Online Safety group have reviewed the appropriateness of our filtering and monitoring system and have:

- identified and assigned roles and responsibilities to manage filtering and monitoring systems
- ensured that our filtering and monitoring system blocks harmful and inappropriate content without unreasonably impacting teaching and learning
- effective monitoring strategies in place that meet their safeguarding needs.

Visiting websites and searching online

Staff must preview sites, software and apps before their use in school or before recommending them to children. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parent/carer permission sought where required. If internet research is set for home learning, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.
When working with pupils searching for images should be done through Google Safe Search (standard through our school connectivity service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.
For more information see our child protection policy.

Storage of Images

Photographs and videos provide valuable evidence of children's achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See privacy notice on the school website for greater clarification).
Staff and Governors (when acting in their governor role) must never use their own devices to take or store

images of children.
At the beginning of every school event parents and carers will be reminded about taking photos for their own personal use and not sharing these on any social media/networking sites.

Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The code of conduct for Staff and Governors includes online safety guidance. The school works with external partners (HfL/NSPCC) to ensure we keep our knowledge and expertise about the safe and appropriate use of internet, mobile and digital technologies up to date. This training is recorded as part of safeguarding records.

New staff are provided with a copy of this policy and the Staff Code of Conduct and must agree to and sign the school's Acceptable Use Agreement (Appendix A.)

Supply staff, trainee teachers and regular visitors/organisations working with children at our school are provided with a copy of this policy.

Home School Triangle

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.
It is important that parents/carers understand the crucial role they play in this process (more information in Appendix C.)

Parents/carers are asked on an annual basis to read and discuss the internet safety poster.

Records, monitoring and review

In the event a child or adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material this must be reported to the Head Teacher or School Business Manager. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously. Where appropriate the Head teacher will make a referral to Children's Services or the police. Any breaches of policy will be recorded on CPOMS.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Appendices

Appendix A: Online Safety Acceptable Use Agreement - Adults
Appendix B: Online Safety Acceptable Use Agreement - Children
Appendix C: Bernards Heath Infant and Nursery School Expectations of Parents and Carers

Appendix A: Online Safety Acceptable Use Agreement - Adults

Internet Access

I will not access or attempt to access any sites that contain any of the following: gambling, child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident and reported to the Head Teacher. Purposeful access of these sites will be managed under the disciplinary policy.

Online conduct

Information about our school expectations about conduct on social media is included in the Staff Code of Conduct.

I understand that it is my responsibility to keep passwords confidential.

Visitors will be given the code for WiFi as appropriate and with authorisation of the Head Teacher.

Images and videos

I will only upload images or videos of staff, children or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices.

I will not use my personal device in front of children.

I will not save secure school information (anything that identifies individual children) on personal devices.

Additional hardware/software

I will not install any hardware or software on school equipment without permission from the Head Teacher

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times, including when setting home learning.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the Head Teacher.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check any sites for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Head Teacher.

Virtual Meetings/Online Teaching

I will only use Microsoft Teams for school related virtual meetings.

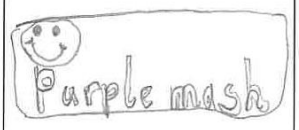
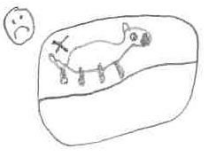
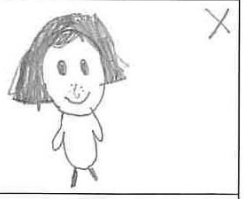
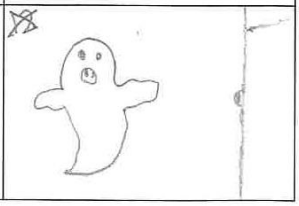
User signature

I agree to follow this Acceptable Use Agreement and to support online safety teaching throughout the school.

Signature …….…… Date ……
Full Name ……..... (printed)
Role within school ……

Rules for learning and playing online and looking after electronic devices.

At school we have iPads and laptops with internet access. We use these devices to help us with our learning. These rules will keep me safe at school and at home.

I will only use equipment for activities agreed by an adult.	
I will only open or delete files when told to by an adult.	
If I see anything upsetting, unpleasant or anything that makes me feel unsafe, I will tell an adult immediately.	
I will not give out information about me, including: my name, school, phone number, home address or clubs I go to. I will tell an adult if anyone asks me online for personal information.	
I will always ask if it is okay to use a picture of me when I am playing or learning online. I will not use pictures of anyone else without their permission or their adult's permission if they are a child.	
I understand that not everything on the internet may be true.	
I understand that I am not allowed to bring electric devices to school.	
I will not play games, watch films or use Apps that are for children older than me.	

Appendix C – Bernards Heath Infant and Nursery School Expectations of Parents/Carers

We want all children to be safe and responsible when learning and playing online. It is essential that home and school work together to teach children about how to be safe online and how to get help/what to do if they are worried/scared/upset about anything they experience.

We ask families to talk about the online safety rules (on previous page) and ensure that children understand their importance and what they mean, at home and at school.

We also ask that parents/carers and visitors to school do not:

- Take photos of on school premises of anyone other than their own child/ren
- Share photos of children taken at school events
- Share school related information
- Post material that may bring the school or any individual within it into disrepute.
- Let their children bring electronic devices to school
- Set up any outward facing site, page, chat group or any other online presence that uses the school name or logo in any form. (This does not preclude setting up class WhatsApp groups.)

We remind parents and carers that rather than posting negative material online about an aspect of school they should talk to the Head Teacher. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

Parents/carers must report any online incidents that cause concern to the Head Teacher. If the incident involves an indecent image of a child the report must also be made immediately to the police. The school will investigate and respond to all reported incidents, liaising with others where appropriate. We ask that parents report to school when other children are involved rather than approaching other parents. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.