



Online Safety Policy

Berkeley Primary School

Policy agreed by Governors	March 2026
Policy uploaded to website	March 2026
Review date	March 2029
Author	Iain Dalgleish Helen Earl Wendy Howlett Anna Cvijetic



Aims and Objectives

- To set out the key principles expected of all members of the school community at Berkeley Primary School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Berkeley Primary School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Introduction

New technologies have revolutionised the movement, access, storage and processing of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Berkeley Primary School, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. Our school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing. However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Online safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks. This policy sets out clearly our expectations of pupils, staff, parents and members of the wider community to ensure best practice.

Scope of the Policy

- This policy applies to the whole school community including Berkeley Primary School's senior leadership team, school board of governors, all staff employed directly or indirectly by the school and all pupils.
- Berkeley Primary School's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision of Online Safety within or related to school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers headteachers, to such an extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other Online Safety-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate Online Safety behaviour that takes place out of school.
- The school will, when necessary, act within the boundaries of the DfE guidance on Searching, screening and confiscating published in Feb 2014.
- This policy should be read in conjunction with the Responsible use of AI policy.



Review and Ownership

- The school has appointed Online Safety Leaders who will be responsible for document ownership, review and updates: Mrs Cvijetic and Mr Dalglish are joint Online Safety leaders.
- The Online Safety policy has been written by the school Online Safety Leaders and is current and appropriate for its intended audience and purpose.
- The school Online Safety policy has been agreed by the senior leadership team and approved by governors.
- The Online Safety policy will be reviewed every three years or when any significant changes occur with regard to the technologies in use within the school.
- The School has appointed a member of the governing body to take lead responsibility for Online Safety. This is the Safeguarding governor.

Communication

- Berkeley Primary School's senior leadership team will be responsible for ensuring that all members of school staff and pupils are aware of the existence and contents of the school Online Safety policy and the use of any new technology within school.
- The Online Safety policy forms part of the school induction process.
- Online Safety leaders within school will be responsible for auditing/reviewing the Online Safety policy annually.
- Pertinent points from the school Online Safety policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the Online Safety policy will be reflected and consistent within all Acceptable Use Policies in place within school.
- We endeavour to embed Online Safety messages across the curriculum whenever the internet or related technologies are used.

Responsibilities

Responsibilities of the Online Safety Leaders

- To promote an awareness of and commitment to Online Safety throughout the school.
- To take day-to-day responsibility for Online Safety within school and to have a leading role in establishing and reviewing the school Online Safety policies and procedures.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated governor.
- To develop an understanding of current Online Safety issues, guidance and appropriate legislation.
- To ensure that Online Safety education is embedded across the curriculum.
- To ensure that Online Safety is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To ensure that Online Safety incident logs are recorded on CPOMS.
- To work closely where appropriate with the designated Child protection coordinator.
- To ensure that any child protection related issues are reported in accordance with school policy.

Responsibilities of teachers and support staff

- To read, understand and help to promote the school's Online Safety and Responsible use of AI policies and guidance.
- To have read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem in accordance with school policy.
- To develop and maintain an awareness of current Online Safety issues and guidance.
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems.
- To embed Online Safety messages in learning activities across the curriculum.



Berkeley Primary School Online Safety Policy



- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and of legal issues relating to electronic content, such as copyright laws.
- To understand and be aware of incident-reporting mechanisms that exist within the school.

Responsibilities of pupils

- To read, understand and adhere to the school's Pupil Acceptable Use Policy.
- To help and support the school in the creation of Online Safety policies and practices (consultation e.g. School council and online surveys) and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile communication devices, digital cameras and handheld devices.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely, both in school and at home.
- To understand what actions they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online Safety issues with family and friends in an open and honest way.

Responsibilities of parents and carers

- To help and support the school in promoting Online Safety.
- To read, understand and promote the school's Pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To consult with the school if they have any concerns about their children's use of technology.
- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's Online Safety and Responsible use of AI policies and guidance.
- To have read, understood and adhere to the applicable Acceptable Use Policy.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils as part of the wider ICT and safeguarding strategies of the school.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To ensure appropriate funding and resources are available for the school to implement its Online Safety strategy.



Responsibilities of the Designated Senior Lead for Safeguarding

- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming and sexual exploitation of children and young people
- To be aware of and understand cyberbullying and the use of social media for this purpose.
- To ensure the school is compliant with the DFE standards for Filtering and Monitoring.

Digital Images

Digital still and video cameras and tablets are used to take pictures of special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a media consent form.

On the website and Class Dojo, we never state a child's full name with their image. The school will happily remove any image of a child on the school website, the school app or Class Dojo at their parents' request.

Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. Pupils are taught not to copy or share any images of themselves or other children produced in school.

- Written permission from parents or carers is obtained before photographs of pupils are published.
- Parents and carers may withdraw permission, in writing, at any time.
- We will remind staff and pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind staff and pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Staff and pupils will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices.
- Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online with the exception of closed platforms such as Google Classroom; such resources will not be published online without the permission of the staff and pupils involved.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social-networking sites.
- When searching for images, video or sound clips, pupils in Key Stage 2 will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network, School tablet devices or within Google Drive/Google Photos and never transferred to personally-owned equipment.
- Staff should regularly review the images they have stored and delete them as soon as they are no longer necessary.



Teaching and Learning

- We will provide specific Online Safety-related lessons in every year group (Nursery to Year 6) as part of the computing curriculum /PSHE curriculum /other lessons.
- Our Online Safety Curriculum is guided by [Teaching online safety in school \(DFE, 2019\)](#) and [Education for a Connected World framework \(DFE, 2020\)](#).
- We will celebrate and promote Online Safety, including promoting Safer Internet Day each year.
- We will ensure that all staff are aware of the latest developments regarding Online Safety and that this awareness is modelled within their lessons.
- We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil agrees to.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and, in age appropriate ways, to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All Pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

Our staff receive regular information and training on Online Safety issues in the form of annual safeguarding training.

- As part of the induction process all new staff receive information and guidance on the Online Safety policy and the school's staff Acceptable Use Policies.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are vigilant with regard to monitoring behaviour changes that may be as a result of new technology or online games being launched.

Internet Access

- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate. This should be incorporated into the Home School Agreement.
- A process exists to have access granted when all the necessary documentation has been completed.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.



Berkeley Primary School Online Safety Policy



- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- Infant pupils' internet access will be directly supervised by a responsible adult.
- Junior pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe use.
- A process is in place to have internet access removed should it become necessary. We will follow our Behaviour Policy if necessary.

Filtering and monitoring

The school adheres to DfE guidance on Filtering and Monitoring.

- The school uses a filtered internet service.
- The school's internet provision will include filtering appropriate to the age and maturity of students.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the applicable Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the DSL. All incidents should be documented under the 'Safeguarding' > 'E-Safety' categories on CPOMS.
- If users discover a website with potentially illegal content, this should be reported immediately. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, [CEOP](#), the [IWF](#) or [The Home Office](#).
- The school will regularly review the filtering product for its effectiveness.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Students will be taught to assess content as their internet-use skills develop.
- Students will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- A digital monitoring system is in place on pupil devices. The SLT and Safeguarding lead are alerted daily to escalated incidents and these are acted on promptly, in line with this policy and our Behaviour policy. These are logged on CPOMS as appropriate.
- Staff remain vigilant and physically monitor pupils' use of technology. They ensure they can see what pupils are doing on devices.
- Laptops or other school hardware can be requested by the technician or SLT at any time.

Email and Google Workspace for Education

Staff, Governors and pupils are provided with a school email account which is managed through Google Workspace for Education (previously GSuite for Education). This is required for teaching and learning in line with the school's Computing policy. All accounts are organised into 'Organisational Units' allowing settings to be tailored to the users' needs. When a child leaves, the account is deleted. When a member of staff or governors leaves, the accounts will be reviewed, relevant folders kept and then the account closed.

Some pupils will have their own personal email accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for their usage here at school. For this reason, we do not permit the use of personal email accounts by pupils at school or



at home for school purposes. Pupils are taught that using a personal email account in school or for school use is not permitted.

All stakeholders

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils, staff and governors may only use school-provided email accounts for school purposes.

Staff and governors

- Emails containing personal, confidential, classified or financially-sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Staff and governors will be reminded about the dangers of revealing personal information within email conversations.
- Staff and governors will be reminded when using email about the need to send polite and responsible messages.
- The school gives all staff and governors their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff and governors must not reveal personal details of themselves or others in email communications to external third parties without fully understanding the need to do so.
- Staff and governors will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Staff and governors will only use official school-provided email accounts to communicate with pupils and parents and carers.
- Under no circumstances should staff and governors contact pupils, parents or conduct any school business using personal email addresses.
- Communication between staff, governors and pupils or members of the wider school community should be professional and related to school matters only.
- Staff and governors will be made aware of email scams to prevent information being shared with someone masquerading as a trustworthy entity or a legitimate person or business.
- Staff and governors should never open attachments from an untrusted source but should consult the network manager or Online Safety Leader first.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to the Online Safety Leader and logged as an incident immediately.
- Irrespective of how staff and governors access their school email (from home or within school), school policies still apply.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- All emails that are no longer required or of any value should be deleted.
- Email accounts should be checked regularly for new correspondence (daily) during work time.
- When away for extended periods, 'out-of-office' notifications should be activated so that colleagues are aware that you are not currently available.
- Staff and governors should not forward work-related emails on to personal email addresses.
- School-owned information should not be attached and forwarded to a personal email address as a means of data transfer.



Pupils

- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils have their own accounts and should only ever log in as themselves.
- Pupils are given a generic password to access their account. When pupils reach UKS2, they are taught about password security and encouraged to change their passwords.
- Access to emails (Gmail) is switched off for all pupils by default. When pupils are learning about email or require access to their email account for curriculum purposes, this will be turned on for the specific organisational unit/year group.
- Pupil accounts are restricted to send and receive emails within the school domain (to and from those with a Berkeley Primary School account) only.
- Pupils will be reminded when using email about the need to send polite and responsible messages.
- Pupils will be reminded about the dangers of revealing personal information within email conversations.
- Pupils must not reveal personal details of themselves or others in email communications.
- Pupils will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- Pupils should never open attachments from an untrusted source but should consult the network manager or appropriate adult first.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All emails should be written and checked carefully before sending.
- Pupils are given access to Google Classroom and Google Drive (including related programs) as deemed necessary by the Computing Coordinator.
- Pupils should use their account only for school related purposes.
- Pupils should communicate sensibly and respectfully when using their account.

Data security and passwords

Staff should ensure that all login credentials (including passwords) are not shared, displayed or used by any other person. The use of password managers can support staff to remember longer passwords. They will ensure they use strong passwords and will change these if they have reason to suspect these are known to others or are instructed to do so by the IT technician, SLT or Computing Leader.

Multi-Factor Authentication

Staff members may be asked to set up multi-factor authentication (MFA) as a requirement to access school systems. In addition to a password, authentication methods may include use of an authentication app on a personal mobile phone or another device, such as a USB security key, or a one-time code sent to a phone.

Copyright

Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. No images downloaded from the internet should be placed on the school website or app. We expect all users to respect copyright laws.

It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information.



Publishing content online

We use the school website and the Class Dojo app to publish content online to enhance the curriculum by providing learning and teaching activities that allow students to publish their own content. However, we will ensure that staff and students take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by students will take place within the school website / dojo app.
- Students will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- All public-facing materials created by students will be moderated by the appropriate member of staff prior to being published.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Accounts and access to other online services

Where the school deems it necessary, pupils are provided with accounts for other websites, services or apps. These include but are not limited to: Times Tables Rock Stars / Numbots; ~~Bug Club~~; Lexia; Prodigy; Band Lab; Scratch; Canva; Spelling Shed; TinkerCad; Anton. Staff carefully scrutinise and select sites that add educational benefit. Our GDPR policies are followed.

Where pupils have been provided with individual accounts, pupils must:

- Only log in using their own account.
- Keep their login details private.

Social networking

Staff and governors

- Staff and governors must not talk about their professional role in a personal capacity when using social media and digital communication tools (such as Facebook, Twitter/X, YouTube, Messenger, WhatsApp, Instagram, TikTok or any other online publishing websites). They must not write anything that would bring myself or the school into disrepute.
- If interacting with professionally related social media (i.e. education forums on apps such as Twitter, Facebook and Instagram) they must not write anything that would bring themselves or the school into disrepute or that could result in a data breach.
- Staff and governors must not use social media platforms or digital communication tools to discuss or share personal information relating to school that could result in a data breach.
- Staff and governors must not use social media tools to communicate with current or former pupils under the age of 18 unless prior permission has been granted by the headteacher.
- Staff and governors must not request, or respond to any personal information from a child or parent, ensuring that communication only takes place within clear and explicit professional boundaries through the school's own communication channels.
- Staff and governors are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.
- Staff and governors will not use any social media tools to communicate with parents unless approved in writing by the headteacher.
- Staff and governors must report any incidents of cyberbullying to the school Designated Senior Lead for Safeguarding.
- Staff will raise any concerns about pupil use of social media sites with parents/carers. The school will regularly remind parents of age ratings of apps/websites through online safety updates published on the school website.



Berkeley Primary School Online Safety Policy



- Social media sites will not be used during teaching time or in sight of pupils without prior permission of the headteacher.
- Staff and governors must not share images or video of any school organised social events on social media sites.

Pupils

Berkeley Primary School will advise pupils of age restrictions on social media sites but recognise that parents may have permitted children to use the sites. As such, Berkeley Primary School:

- Will block/filter access to social networking sites and newsgroups, unless a specific use is approved.
- Will advise pupils never to give out personal details of any kind which may identify them and /or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Will advise pupils not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupils or his/her location e.g. house number, street name or school.
- Will advise pupils on security and encourage them to set passwords, deny access to unknown individuals and instruct them on how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Will advise pupils not to publish specific and detailed private thoughts.
- Should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Will ensure pupils know how to report incidents of cyber bullying and inappropriate content.

Parents

- Parents will be reminded of their responsibilities in relation to the use of social media via notices given at the beginning of school events.
 - Parents will be reminded that images and video taken of children at school events are for personal use only and not to be published online.
- Parents are made fully aware of the correct escalation process for concerns or complaints and that social media is not an appropriate forum for such issues.

Cyberbullying

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyberbullying is the use of any media to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy.

Bullying of any type will not be tolerated by the school and will be dealt with under the school's procedure. Berkeley Primary School:

- Fosters a 'No Blame' environment that encourages pupils to tell a responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Ensures pupils and staff know what to do if they find inappropriate web material.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident.
- Ensures pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK
 - to understand 'Netiquette' behaviour when using an online environment / email, i.e.



Berkeley Primary School Online Safety Policy



be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission.

The School Website

- The school website will not include personal details, including individual email addresses or full names of pupils.
- A generic contact email address will be used for all enquiries received through the school website.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

Mobile Communication Devices (including mobile phones)

Pupils are not permitted to have mobile communication devices upon their person in school. We recognise that our older pupils may walk on their own to and from school and parents may wish them to have a mobile communication devices for emergencies; any device brought in must be handed to the office for the duration of the day.

We accept that most staff will own a mobile communication device and have one in their possession during the school day. They may be used during breaks when not supervising children.

- Personal mobile communication devices will not be used or visible when supervising children without prior consent from SLT or for Multi Factor Authentication. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile communication devices.
- No images or videos should be taken on personal mobile communication devices without the prior permission from the headteacher or SLT member (permission may be given when on school visits, activities, etc). Any images must be deleted from the device within 24 hours
- Staff are permitted to use their own mobile devices for contacting children, young people or their families within or outside of the setting in a professional capacity but must ensure their own personal number is withheld.
- Mobile phones may be used to authenticate logins using approved 2-factor authentication apps or access one-time codes where a school system requires it.
- In exceptional circumstances, staff may be contacted via their personal device and SLT may be contacted.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Staff will not allow students to use their personal mobile communication devices for good behaviour.

Physical Safety

All electrical equipment in the school is tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum. We expect pupils to behave appropriately near electrical sockets and appliances.



All the projectors in our school have maximum light levels below the government's health and safety guidance of 1,500 ANSI lumens. Pupils are taught that they should not look directly at strong light sources such as the sun, lasers or data projectors. We expect all users to not look directly into the light beam when working on the interactive whiteboards.

Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. We expect all users to refrain from eating and drinking when working at a computer.

Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. We expect all users to take responsibility for their own physical wellbeing by adopting good practices.

Computers and other ICT equipment can be easily damaged. Pupils are taught the correct way to use ICT equipment. We expect pupils to respect ICT equipment and take care when handling and using.

Pupil devices are stored in charging trolleys. These must be moved by or with an adult and care should be taken to avoid injury to themselves or others.

Monitoring

- ~~Monitoring software will be installed on all school owned hardware if deemed appropriate.~~
- ~~All school email, internet, systems, platforms and network usage is monitored and logged.~~
- ~~Laptops or other school hardware can be requested by the technician or SLT at any time.~~
- ~~It will be the responsibility of the DSL (Designated Safeguarding Lead) and Online Safety leader to manage the monitoring system within school for Online Safety related incidents.~~
- ~~All data created within the monitoring system will be resilient and backed up accordingly, so evidence can be preserved should it become necessary.~~
- ~~Children will not use IT equipment unless supervised by a member of staff~~
- ~~All concerns will be dealt with in line with the school's safeguarding procedures and raised with the DSL.~~

Responding to incidents

- All Online Safety incidents, including internet misuse, should be reported to the DSL in line with school policy.
- CPOMS should be completed and escalated to the relevant person within school.
- Complaints of a child protection nature must be dealt with in accordance with the school policy.

Online Complaints

- Parents/Carers are reminded through information on the school website of appropriate complaints channels and procedures.
- All staff and governors are aware of how to report any negative online comments about the school or members of the school community.
- Staff and governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the headteacher.



Appendix 1 - Acceptable Use Policy (Pupils) - letter

Date

Dear Parents / Carers,

As part of our curriculum enhancement and the development of computing skills, Berkeley Primary School is providing supervised access to the internet.

Pupils may exchange email with partner schools, research information and visit websites as part of their programme of learning.

We have purchased our internet access from an educational supplier that operates a filtering system that restricts access to inappropriate materials. Computers and tablets are always used within view of school members of staff and the children's access is supervised.

We ask that you read and discuss the enclosed acceptable use policy with your child. These rules have been developed to help teach your children how to stay safe online and to use ICT equipment responsibly. The children have already discussed them in school and have signed to say that they will abide by the rules. It is, however, very important that these rules are also reinforced by parents / carers at home. We regularly discuss these rules in school with the children as part of our teaching.

If you wish to discuss any issues associated with internet use, please do not hesitate to speak to your child's class teacher.

Yours sincerely,

Anna Cvijetic
Headteacher



Appendix 2: AUP - pupils

Pupil Acceptable Use Policy

This document has been developed to help you understand the rules of using ICT in our school. You should always follow the rules set out in this policy because they will help to keep you and your friends safe.

- I will look after school ICT equipment and use it properly.
- I will not eat or drink near ICT equipment.
- I will only use the internet when a school member of staff says I can.
- I will only use the school's computers, tablets and Chromebooks for my school work / homework.
- I will only log into computers, apps or websites as myself.
- I will not access other people's files or accounts.
- I will not bring in a memory stick from outside school unless I have been given permission.
- If I see something that I feel uncomfortable with I will tell a school member of staff straight away and
 - o turn off the monitor on a desktop computer.
 - o lock the tablet if using a tablet.
 - o minimise the window if using a Chromebook or laptop.
- I will report any unpleasant material or messages sent to me to a trusted adult in school.
- I will treat my Google Classroom like my real classroom, only posting messages that are kind, polite and useful.
- I will only use email when I have been told to by my teacher and the messages I send will be polite and responsible.
- I will only email people I know and / or that my teacher has approved.
- I will not give out personal information including my home address or phone number.
- I will not arrange to meet someone that has been talking to me online.
- I understand that the school may check my files and ~~may~~ will monitor the internet sites I visit.
- I will not try to get on any websites that my school has blocked access to.
- Whilst at school, I will only use a mobile phone or other mobile device if school members of staff say that I can. I will not use it on the school site.

I have read and understood the acceptable use policy. I will follow these rules in order to stay safe.

Date

.....

Pupil's signature

.....

Pupil's name

.....

Class



Appendix 3- Acceptable Use Policy (staff, governors, students, volunteers)

BERKELEY PRIMARY SCHOOL Acceptable Use Policy (AUP)

I understand that I must use school and personal ICT systems in a responsible way, to ensure that there is no risk to my professional role, safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, wherever possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

- I will only use the school's digital technology resources and systems for appropriate professional purposes relating specifically to my role and responsibilities or for uses deemed 'reasonable' by the Head and Governing Body.
- All ICT must be password protected to access the device.
- I will only use the school approved file storage for any school data.
- I will use the school approved email system for written communication with other staff.
- I understand that I may be required to use authentication apps or receive authentication messages to my personal devices.
- I understand that The Data Protection Act (2018) requires that any information seen by me with regard to staff or pupil information, held within any schools' system (e.g. MIS, Learning Platforms etc), will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Senior Leadership Team (email) and, if related to a child accessing, log this on CPOMS (Under 'Safeguarding' > 'E-Safety').
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure that all my login credentials (including passwords) are not shared, displayed or used by any other person.
- I will ensure I use strong passwords and will change these if I have reason to suspect these are known to others.
- When leaving a laptop, computer or other device unattended, I will ensure it is locked or switched off.
- All school devices will be switched off overnight.
- I will ensure school systems (i.e. Arbor, Insight, CPOMS, email account) are not displayed for children to see on devices (i.e. on big screens, IWB or unattended laptops/tablets).
- Personal mobile communication devices will not be used or visible when supervising children without prior consent from SLT or for Multi Factor Authentication. They should be switched off or silent at all times.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured appropriately.
- I will ensure that any external storage devices are kept secure at all times and personal data is encrypted. The google drive should be used for storage wherever possible and for transferring data from one device to another.
- All school-owned devices will only be used for school related business and professional use and I will not allow family members to use school-owned equipment.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will ensure that my personal email accounts, mobile/home telephone numbers are not shared with pupils or families.
- I will not use social media tools to communicate with current or former pupils under the age of 18 unless prior permission has been granted by the headteacher.



Berkeley Primary School Online Safety Policy



- I will not request, or respond to any personal information request from a child or parent, ensuring that communication only takes place within clear and explicit professional boundaries through the school's own communication channels.
- 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 not visit sites or use social media in a way that may appear to encourage, justify or glorify terrorist violence in furtherance of particular beliefs; seek to provoke others to terrorist acts; encourage other serious criminal activity or seek to provoke others to serious criminal acts; foster hatred which might lead to inter-community violence.
- I will not talk about my professional role in a personal capacity when using social media and digital communication tools (such as Facebook, Twitter/X, YouTube, Messenger, WhatsApp, Instagram, TikTok or any other online publishing websites). I will not write anything that would bring myself or the school into disrepute.
- If interacting with professionally related social media (i.e. education forums on apps such as Twitter, Facebook and Instagram) I will not write anything that would bring myself or the school into disrepute or that could result in a data breach.
- I will not use social media platforms or digital communication tools to discuss or share personal information relating to school that could result in a data breach.
- I understand that all school email, internet, systems, platforms and network usage is monitored and logged and this information could be made available to the senior leadership on request. Laptops and other school hardware can be requested by the technician or SLT at any time.
- If I connect a computer, laptop or other device (including USB flash drive), to the network / Internet that has not been approved by the school, I must ensure it meets minimum security specification. (i.e. up to date approved anti-virus etc.)
- I will not use personal digital cameras or camera phones to take and store images of pupils or staff without permission from the Headteacher or SLT member (permission may be given when on school visits, activities, etc). Any images must be deleted from the device within 24 hours.
- I will regularly review the files and information (including photographs) I have saved and delete that which is no longer necessary.
- I will ensure that I am aware of digital safeguarding issues so they are appropriately embedded in my own and classroom practice.
- I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will not enter any personal information (personal data, pupil photos, intellectual property or private information including commercially sensitive information, such as contracts) into any Generative AI model.
- I will not allow generative AI tools to use data I have entered, including work created by pupils, to further develop, train or enhance the model (feedback-loop).
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the Headteacher immediately.
- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use and Online Safety Policies. You will be asked to confirm you have read the most up to date version of this annually (as part of the annual safeguarding training).

Signature Date

Full Name(printed) Job Title



Appendix 4 What to do if?

Staff should follow the following guidelines in the event of an e safety incident:

An inappropriate website is accessed unintentionally in by a child, young person or member of staff.

1. Play the situation down; don't make it into a drama.
2. Report to the Headteacher/Designated Senior Lead and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses school IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the Headteacher should then:
 - Remove the PC to a secure place.
 - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the academy.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (contact Personnel/Human Resources).
 - Refer the incidence to the Local Authority Designated Officer (LADO)
 - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
 - Contact the local police or High Tech Crime Unit and follow their advice.
 - If requested remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant LSCB policies and procedures including what to do if you are worried, e-safety antibullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.



You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in the school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement of the police and children's services.
5. Inform LA e-safety officer who is The Head of Safeguarding and Practice
6. Consider delivering a parent workshop for the academy community.

All of the above incidences must be reported immediately to the Headteacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.