Beenham Primary School

POLICY DOCUMENT
Digital Safety Policy

Aims

Our school aims to:

Have robust processes in place to ensure the digital safety of pupils, staff, volunteers, and governors.

Deliver an effective approach to digital safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones') Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to digital safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.

Contact – being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and

deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss digital safety (via CPOMS reporting function) as provided by the designated safeguarding lead (DSL).

The governor who oversees digital safety is the Safeguarding Governor.

All governors will:

Ensure that they have read and understand this policy.

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

Ensure that digital safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.

Ensure that, where necessary, teaching about safeguarding, including digital safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Leaders

Details of the school's designated safeguarding lead (DSL) and deputy (DDSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL and DDSL takes lead responsibility for digital safety in school, in particular:

Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Working with the headteacher and other staff, as necessary, to address any digital safety issues or incidents.

Managing all digital safety issues and incidents in line with the school safeguarding policy.

Ensuring that any digital safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.

Updating and delivering staff training on digital safety.

Liaising with other agencies and/or external services if necessary.

Providing regular reports on digital safety in school to the Safeguarding Governor.

This list is not intended to be exhaustive.

The ICT link governor

The ICT link governor alongside the Headteacher is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

Conducting a full security check and monitoring the school's ICT systems on a termly basis.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Ensuring that any digital safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy.

Implementing this policy consistently.

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).

Working with the DSL to ensure that any digital safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Class Dojo. This policy will also be shared with parents.

Digital safety will also be covered during parents' evenings where required.

The school will let parents know:

What systems the school uses to filter online use – *We buy into West Berkshire provided services to provide our firewalls.*

What their children are being asked to do online, including the sites they will be asked to access to support their learning – *these can be found on the class web pages.*

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DDSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or

- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DDSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or undermine the safe environment of the school or disrupt teaching, and/or Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if.

They reasonably suspect that its continued existence is likely to cause harm to any person,

and/or the pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL/ DDSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Appendix 1

Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

Pupils using mobile devices in school

Pupils who walk home alone, may bring mobile devices into school, but are not permitted to use them during:

- Lessons.
- Clubs before or after school, or any other activities organised by the school.
- All devices must be handed into the school office on arrival and collected at the end of the day.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Making sure the device locks if left inactive for a period.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages.
- Sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to digital safety via CPOMS.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board.

DATE APPROVED: 15th October 2024	**NEXT REVIEW DATE: November 2024**

Appendix 2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like iPads) and get onto the internet in school I will: Ask a teacher or adult if I can do so before using them. Only use websites that a teacher or adult has told me or allowed me to use. Tell my teacher immediately if: o I click on a website by mistake. o I receive messages from people I don't know. o I find anything that may upset or harm me or my friends. Use school computers for schoolwork only. Be kind to others and not upset or be rude to them. Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly. Only use the username and password I have been given. Try my hardest to remember my username and password. Never share my password with anyone, including my friends Never give my personal information (my name, address, or telephone numbers) to anyone without the permission of my teacher or parent/carer Check with my teacher before I print anything. Turn off an iPad when I have finished using it. **I agree that the school will monitor the websites I visit.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3

- ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

Use them in any way which could harm the school's reputation.

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services.

Install any unauthorised software or connect unauthorised hardware or devices to the school's network.

Share my password with others.

Take photographs of pupils without checking with teachers first

Share confidential information about the school, its pupils or staff, or other members of the community.

Access, modify or share data I'm not authorised to access, modify or share.
Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices and personal devices used for work matters are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the Headteacher or DDSL know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**