Online Safety and Acceptable Use Policy

The Beeches Primary School

Author:	David French
Version:	3
Approval date:	February 26
Next revision date:	February 27
Approving / revision body lead:	DSL / Safeguarding Governor

Contents

The school policy is well established. Changes made between 2024/2025 and 2025/2026 have been highlighted in green to ensure the policy remains well understood by all stakeholders.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- Deliver an effective approach to online 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
- Ensure compliance with Keeping Children Safe in Education 2025, including strengthened expectations relating to online harms, AI-generated content, harmful sexual content, misinformation, disinformation, conspiracy theories, filtering and monitoring, and the safe use of mobile and smart technologies.
- Ensure alignment with the school's AI Policy (2025) and the updated RSHE curriculum (2026), which strengthen expectations around online relationships, digital consent, AI-related harms and media literacy.

The 4 key categories of risk

Our approach to online 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 peer-to-peer 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., consensual and non-consensual 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

2. 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.

This policy also reflects the updated Relationships, Sex and Health Education (RSHE) Curriculum 2026, including strengthened expectations around online relationships, digital consent, self-generated imagery, and harmful online sexual content.

This policy complies with our funding agreement and articles of association.

This policy also reflects updates in Keeping Children Safe in Education (2025), which introduce strengthened guidance on online safety education, including online misogyny, incel-related harms, harmful sexual content, the impact of algorithms, artificial intelligence, deepfakes, manipulation, online financial exploitation, and the increasing risks posed by misinformation, disinformation and conspiracy theories.

Misinformation: False or misleading information shared without intent to cause harm. Example: A pupil sharing a false rumour online that a celebrity has died because they believe it to be true.

Disinformation: False information that is deliberately created or shared to cause harm, manipulate opinions or influence behaviour. Example: A social media post intentionally spreading a fake story claiming a local school is unsafe to influence public opinion.

Conspiracy theory: An explanation for events that falsely suggests a secret plot by powerful groups, often without evidence. Example: Content claiming that natural disasters are secretly controlled by the government.

The school's AI Policy (2025) sets out expectations for the safe, ethical and age-appropriate use of artificial intelligence tools and technologies by staff and pupils. This Online Safety Policy should be read alongside the AI Policy, particularly with respect to data privacy, deepfake risks, algorithmic bias and the use of generative AI in teaching and learning.

3. Roles and responsibilities

3.1 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 online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Gavin Bateman.

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 online 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 online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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
- Ensure the school's filtering and monitoring systems meet KCIES 2025 expectations, including: regular review, evidence-based assessment of effectiveness, alignment to the school's online safety risk assessment, and clear communication to parents and pupils.

3.2 The headteacher

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

3.3 The designated safeguarding lead

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

The DSL along with the online safety lead takes responsibility for online 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Keep up to date with online harms identified in KCIES 2025, including AI-generated imagery and deepfakes, targeted algorithms, harmful sexual content, misogynistic and incel-related material, self-generated imagery, scams, online fraud, misinformation, disinformation and conspiracy theories.

This list is not intended to be exhaustive.

3.4 IT Support/Broadband Provider.

The IT Support Provider 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The DSL and Online Safety Lead are responsible for:

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy (appendices 4 and 5)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Monitoring use of devices through School Cloud

This list is not intended to be exhaustive.

3.5 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 online safety incidents are logged and dealt with appropriately in line with this policy (appendices 4 and 5)
- 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' use (appendices 4 and 5)
- Ensure no photographs or videos of pupils are created on personal devices or shared externally.

This list is not intended to be exhaustive.

3.6 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 system
- Follow the school rule that prohibits taking or sharing images of pupils externall and internet (appendices 1 and 2)

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

3.7 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).

Visitors must not take photographs or videos of pupils under any circumstances.

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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
- that the school does not permit any external sharing of pupil images for safeguarding reasons.

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
- AI-related online risks, including manipulated media and deepfakes · How algorithms shape online content, including potentially harmful targeted recommendations · Online misogyny and incel-related communities, and how to report harmful sexual content · Recognising and reporting financial scams, phishing attempts and fraudulent behaviour · Understanding misinformation, disinformation and conspiracy theories (with age-appropriate examples)
- Misinformation – When someone shares something untrue because they think it is true. Example: A made-up news story saying a game is being banned in the UK.

- Disinformation – When false information is created or shared on purpose to trick people. Example: A fake social media account pretending to be a teacher and posting false messages.
- Conspiracy theories – When people claim something secret or hidden is happening without real evidence. Example: Videos claiming that computer games are designed to control children's minds

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.

From September 2026, online safety teaching will reflect updates in the revised RSHE curriculum, including: digital consent and boundaries, navigating online relationships safely, understanding the impact of harmful sexual content online, recognising pressure, manipulation or coercion in digital spaces, knowing how to seek help when experiencing online harm. These changes will be embedded across computing, PSHE and RSHE curriculum planning.

5. 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. This policy will also be shared with parents on the school website.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- Parents are not permitted to take photographs or videos of pupils on school premises, during school events or on school visits.

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 DSL.

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

6. Cyber-bullying

6.1 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.

6.2 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, computing, 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 (see section 11 for more detail).

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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) 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.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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

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

7. Acceptable use of the internet and devices in school

7.1 Access to ICT

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. The ICT equipment is stored securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware and will be kept active and up to date.

At Key Stage 1, pupils will access the internet using a class ID and password, which the class teacher supervises. All internet access will be undertaken with a member of staff within the same room.
At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.

Members of staff will access the curriculum network using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils, or other adults, to access the internet through their ID and password. They will always abide by the school Acceptable Use Policy.

7.2 Use of the internet

The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, use of the learning platform, external email or news groups. The school has an obligation to fulfil its Prevent Duty and to ensure that no extremist or terrorist material can be accessed. Access to internet web sites that are unrelated to school business should be restricted to out of school hours and designated breaks and should not leave a web history that through which pupils may access inappropriate content. Where staff are unsure on whether given content is appropriate, they should contact the online safety lead for clarity.

The use of YouTube as a teaching tool is allowed providing staff have vetted the video prior to the lesson to assess that the content is appropriate. Staff should use the freeze screen function when loading the video in case of any adverts appearing that could contravene this policy. Staff may consider using alternative resources such as Britannica Learning and Espresso.

The school expects all users to use the Internet responsibly and strictly according to the conditions set out in the acceptable use policy. 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 (appendices 1 and 2). 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.

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK
- extremist or terrorist material

Sites must not be accessed which contain inappropriate material defined below.

- Personal ads or dating
- Criminal skills or resources
- Internet based peer to peer networks
- Downloads of ringtones, screensavers and games
- Downloads of freeware, shareware or evaluation packages (excepting by authorised persons as designated by the school and in compliance with copyright law)
- Illegal drugs
- Hacking, virus writing or password cracking
- Gambling
- Depiction or avocation of violence or the use of weapons
- Breach of copyrights
- Instant messaging or online chat rooms not directly related to education or educational use.

If inappropriate material is accessed accidentally, users should immediately report this to the head or member of the safeguarding team so appropriate action can be taken.

7.3 Conducting Financial Activities on the Internet

While this policy does not ban the use of the internet for conducting personal financial transactions, e.g., e-banking, we warn against it on school machines. Residual information from such activities can be left on the computer hard drive and could subsequently be accessed by others. Similarly, personal or financial information may be inadvertently recorded by the school's monitoring software. The school or the local authority do not accept any liability for any resulting loss or damage.

7.4 Intellectual Property, Plagiarism and Copyright

Any information copied or downloaded from the internet and then re-presented in any form should acknowledge the source. Any images used should be copyright free. When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

7.5 Images and videos of pupils

The school does not permit any external use, sharing or publication of photographs, videos or digital images of pupils under any circumstances. This includes, but is not limited to:

- School websites
- Social media (school or personal)
- Newsletters
- External platforms or cloud services
- Public displays or promotional materials
- Personal devices
- Any third-party organisations or individuals

This approach ensures pupil safety, protects their identity, and aligns with safeguarding expectations.

Only school-owned devices may be used to create images or videos of pupils, and only where this is necessary for teaching, learning, assessment or internal record-keeping.

All images and videos must be:

- Created only on school-owned devices
- Stored solely on the school's secure cloud system
- Used only for internal educational purposes
- Never transferred, uploaded, or copied to personal devices, personal cloud accounts or external systems
- Deleted in line with the school's data retention schedule and GDPR requirements

Staff must not use personal devices to create images or videos of pupils in any situation, including:

- Residential trips
- Educational visits
- Out-of-hours activities
- Sporting events
- Performances

- Parents and visitors are not permitted to take photographs or videos of pupils on school premises, school visits or during school-led events.

Where remote communication tools (such as Zoom) are used, sessions will not be recorded unless recording is required for internal safeguarding purposes. Any such recordings must be stored securely on the school server and never shared externally.

This policy applies at all times and in all locations where staff and pupils are acting under the responsibility of the school.

7.6 Social networking

Staff and pupils are not allowed to use their personal account on social networking sites, such as Facebook or Instagram in school on school machines. Staff are permitted use their own mobile device during a break using their own data and not on the school wifi..If staff have social networking accounts, we recommend that their profiles are set to private. Staff must not have contact with pupils from our school through social networking sites. Staff should not post or make comments on social networking sites that may be interpreted as negative or harmful to the school, its employees, pupils or the local authority.

Staff must never upload images or videos of pupils to any external platform, including personal or school-run accounts.

7.7 Staff communication through email

All email messages should include a standard disclaimer stating that the content of the email are not necessarily the views of school or the Local Authority. All professional communication should be through your school email and not through social media or texting. Do not release or in any way make available personal details of any colleague or pupil (phone or personal e-mail addresses) through email or the internet.

Children can 'share' work with their teacher via Office Apps. There is an option for the children to add a message. Notifications are received through teachers email accounts. Staff should report any inappropriate comment or children accessing their accounts after at inappropriate times through My Concern.

All communication with parents will be through office@. Emails from parents will be forwarded to you and you can send back your response to office@. It will then be cut and pasted into an office@ email and sent to the parent. Staff and volunteers must not give their personal details such as home/mobile phone number, home or e-mail address to pupils or parents under any circumstances.

Consider the following,

- Do not send a "reply to all" unless it is necessary for all copy recipients to know your response. Mailing lists provide useful groupings to target messages to the right groups of people.
- The expectation is that emails are being sent "to" people who must take some sort of action. The "cc" is for people who need to know about this, others do not need to be included. If you really need to know an email has been received and read, ask for confirmation.
- Think before you forward emails that you have received, it may contain information that is confidential or expressly for you only.
- When answering emails on phones, it can often mean they are shorter, like a text, and can come across as rude or abrupt. Remember **HALT** – hungry, angry, lonely, tired, think before you send an email, it may not come across as you intend.
- Avoid sending out emails after 9pm or before 6am.
- The sending of email that are wholly or substantially unrelated to school business should be restricted to out of hours and designated breaks and not completed using a school email account.

7.8 Staff use of personal mobile phones

Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, they can use their own devices if they 'withhold' their own mobile numbers for confidentiality purposes. This is done by preceding the telephone number with the digits 141 before calling, e.g. 14101733123456. This will prevent the caller's number being displayed on the receiving phone.

Personal mobile devices should **never** automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces.

Please refer to Policy on the use of mobile phones and other devices in school.

8. Pupils using mobile devices in school

Pupils are not permitted to bring personal devices to school. Where a request for pupils to bring a mobile phone to school for their safety travelling to and from school, the phone should be left with the school office and placed in the safe.

9. 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)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates
- USB devices are not to be used due to security and virus threats.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 DSL.

10. 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 policy for behaviour. When an incident is detected through School Cloud, a member of the safeguarding team will determine appropriate action to support teachers. 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 policies. 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.

11. 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 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
    - Non-consensual 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
- Understanding risks associated with AI-generated content and deepfakes · Awareness of online misogyny, incel communities and harmful sexual content trends · The role of algorithms in shaping pupils' online experiences · Recognising misinformation, disinformation and conspiracy theory content and responding effectively · Identifying financial scams, grooming patterns and online fraud
- Training will also incorporate the updated RSHE curriculum (2026), ensuring staff understand how to teach digital consent, online relationships, self-generated images and harmful sexual content in an age-appropriate manner.

The DSL and deputies 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 child protection and safeguarding policy.

12. Filtering and Monitoring arrangements

The school's approach to filtering and monitoring aligns with the strengthened expectations in KCIES 2025, ensuring systems are:

· Age-appropriate and tailored to pupil need · Regularly reviewed for effectiveness, with findings feeding into the annual safeguarding risk assessment · Clearly understood by staff, parents and pupils · Capable of identifying emerging online risks including misinformation, disinformation, conspiracy theories, AI-generated content and harmful sexual content.

The school will provide clear information to pupils and parents about what filtering and monitoring systems are in place, what they block or flag, and how monitoring alerts are assessed and escalated.

Filtering

- The School uses Talk Straight filtering.
- There are 2 levels for all pupils and for staff and visitors.
- All pupils in KS2 and staff have an IDIP address which can be monitored.

- KS1 pupils have an IDIP address per class.

Monitoring

- All staff are responsible for supervising use of devices in class.
- Pupils are given prechecked apps and websites to use during lessons.
- Staff will circulate the room to maintain awareness of how devices are being used.
- School Cloud is used to monitor activity and picks up trigger words.
- This is monitored daily by a team of staff for both pupil and staff use.

Reporting

- All concerns will be reported on My Concern.
- Staff should be aware of children susceptible to online grooming.
- Any access of inappropriate material, that has got through the filtering, should also be reported to the DSL.
- All staff log behaviour and safeguarding issues related to online safety on My Concern.

This policy will be reviewed every year by the safeguarding team. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Policy on the use of mobile phones and other smart devices in school
- · AI Policy (2025) – safe and appropriate use of artificial intelligence tools by pupils and staff.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

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 computers) 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:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ 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
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
• Not take photos or videos of other children at school.
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

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 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to, or post any material that is offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision • Take, share, or upload photos or videos of other pupils or staff. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

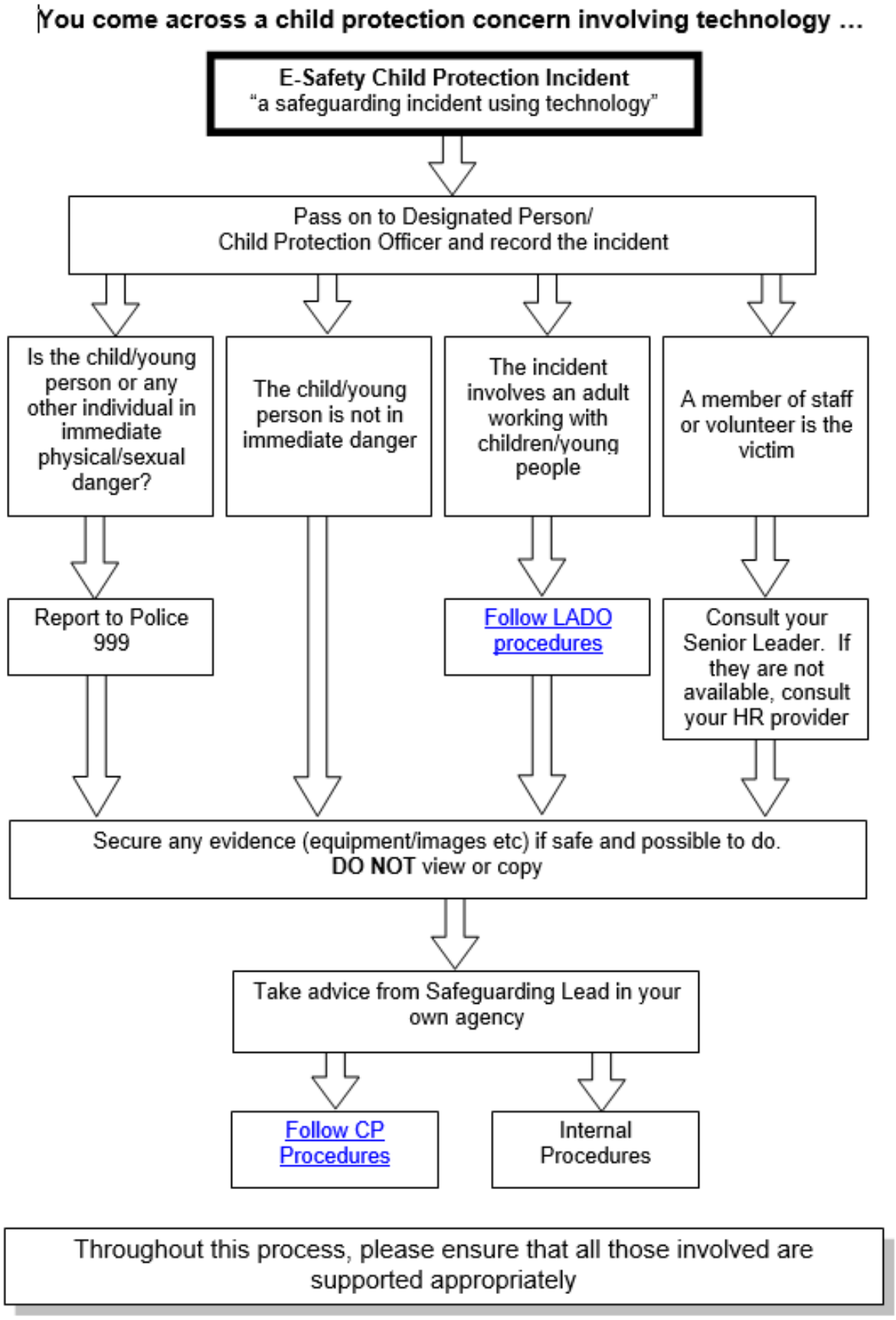
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

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 or log in to the school's network using someone else's details • Take photographs or videos of pupils on personal devices or share pupil images externally under any circumstances. • 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 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 designated safeguarding lead (DSL) 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:**

Appendix 4: Guidance for reporting incidents

Incidents of concern must be reported on My Concern.

If you find inappropriate or illegal material on a PC or other electronic device in school, do not try to capture or copy evidence, this may leave you in the position of distributing illegal images. Ensure pupils cannot access the inappropriate or illegal material - turn off the screen, remove the device to a secure place or switch off power at the wall. You then **MUST** report this to the DSL or safeguarding deputies.



Appendix 5: Guidance when reporting on My Concern

Reporting Online safety concerns guidance

Ask the child questions to gather as much information as possible:

- What app/game were you playing?
- Do you use a chat feature while you are playing? If yes, who do you talk to? Do you share pictures/videos?
- Are you using your own device or your parents/siblings etc?
- Does your parent/carer know your password?
- Do you play/use this while adults are in the room?
- Do your parents/carers know you have an account for this game/app?
- When do you play this game and where? (e.g. are they alone in their bedroom?)
- How often do you play/use this app?
- What would you do if you saw or heard something that you didn't like?

Consider what is the concern related to…

Content

- Illegal
- Inappropriate/disturbing
- Obsession/addiction
- Expense – gambling/advertising/auctions

Contact

- Bullying
- Abuse
- Identity theft
- Grooming

Conduct

- Privacy issues
- Digital footprint/tattoo
- Health & wellbeing
- UGC (user generated content)
- Sexting
- Copyright
- Live streaming