Balfour Infant School

Online Safety Policy

Date **September 2025**

Review Date **September 2026**

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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Ensure all guidance provided by KCSIE 2025 is adhered to.

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, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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.
- Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Responsibilities

The Designated Safeguarding Lead (DSL) including the Deputy DSLs take lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Safeguarding and Child Protection Policies
- 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 and induction on online safety in line with recommendations in KCSIE 2025
- Liaising with other agencies and/or external services if necessary
- Ensuring the school has effective and regular filtering and monitoring systems in school in line with KCSIE 2025 and these are reviewed regularly as well as responding to adhoc incidents
- All related policies are adhered to such as the Remote Learning Policy, Anti-Bullying Policy, Child-on-Child abuse Policy, Acceptable Use Policy and the Code of Conduct policies.

The DSL and Deputy DSLs 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 on the subject of

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 annual safeguarding training. More information about safeguarding training is set out in the school's Safeguarding and Child Protection Policy.

The ICT Support 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
- Alongside the DSL, conducting a full security check and monitoring the school's ICT systems Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Governors are responsible for

- Ensuring that staff to undergo regular updated safeguarding training, including online safety.
- Ensuring that children are taught about how to keep themselves and others safe, including online. Ensuring that online safety is reflected in curriculum planning, training and policies including parental engagement.
- Ensuring the school has appropriate filtering and monitoring systems in place and regularly review it's effectiveness.

All staff are responsible for:

- Maintaining an understanding of this policy
- Having an awareness that technology is a significant component in many safeguarding and wellbeing issues.
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet
- Ensuring that pupils follow the school's e-safety rules
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying and child-on-child abuse are dealt with appropriately in line with the school Behaviour and child-on –child abuse Policies
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline

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. 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 or 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

- An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

The Computing Subject Lead will attend E-Safety training sessions where possible and will keep up to date with initiatives supporting staff to deliver the termly E-safety sessions via Project Evolve.

Training will help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

Pupils:

- E-Safety rules will be displayed in all rooms where workstations are used and these will be discussed with pupils.
- E-Safety will be taught in all year groups as part of Computing and PSHE.
- Pupils will be informed that network and Internet usage will be monitored and appropriately followed up.

Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters or other communications home. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher or the DSL. Concerns or queries about this policy can be raised with any member of staff or the head teacher.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyber bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. 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 procedures within the whole school policy on behaviour, including 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. In an age appropriate manner, the school will 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 within PSHE.

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.

Mobile Phones and smart technology

Staff, pupils and visitors are not permitted to have mobile phones upon their person in school. Staff and visitors are asked to store their mobile phones securely and not use them while pupils are in the room. Pupils are taught that they shouldn't have a mobile phone or smart watch or other smart technology on their person in school.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Balfour Infant School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Balfour Infant School will treat any use of AI to bully pupils very seriously, in line with our antibullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used in school.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

How the school will respond to issues of mis-use

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.

How the Internet will be used

The Internet will be used to enhance children's learning and will include filtering appropriate to the age of the pupils. The school will ensure that the use of internet derived materials by staff and pupil complies with the appropriate copyright laws. When pupils are using the Internet in school they will be closely

monitored. Teachers will use and show pupils how to access safe search engines as recommended by Medway Council.

- Pupils will be given clear objectives for Internet use.
- Pupils will be taught what Internet use is acceptable and what is not.
- E-Safety rules will be visible near all workstations around the school.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught to report any unpleasant content to a member of staff immediately.

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 near the computers. **We expect all users to refrain from eating and drinking when working at a computer.**

- 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.**

- 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 well-being by adopting good practices.**

Network Safety:

- All users need to log on using a username and password. Pupils log on using their year group username. Pupils are taught that they should only access the network using that particular log in. **We expect all users to only logon using their username.**

- Each user is given an allocation of disk space for the storage of their work. Pupils are taught how to save their work into their "My documents" area. **We expect pupils to save and keep their work.**

- Access to other users "My documents" areas are restricted by the network. Pupils are taught not to access another user's work without permission. **We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.**

- On the network there are "shared resource" areas where many different groups of users can save work so that it is available to others. Pupils are taught how to access and save to these shared resource areas. **We expect pupils to respect the contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission.**

- The network software prevents changes being made to computer settings. Pupils are taught that making changes may prevent the computer from working properly. **We expect all users to make no attempt to alter the way the computer is set up.**

- Only the network administrators are permitted to install software on to computers. Pupils are taught that the network or an application may not function properly if programmes are installed. **We expect all users to make no attempt to load or download any programme onto the network.**

- All users of the network can be monitored remotely by the network administrators. Pupils are taught that their use of the network can be monitored. **We expect all users to understand that their use is subject to monitoring.**

Internet Safety:

- When using a network workstation all access to the Internet is protected by a number of different filters via the Medway Council 'Atomwide' approved infrastructure. These filters are designed to prevent accidental or deliberate access to unsuitable materials. Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer. **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.**
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. **We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.**
- The school website contains school policies, newsletters and other information. **We expect all persons accessing the school web site to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

Email Safety:

- Year 2 classes are able to use their class email address facilities which pupils can use for sending messages to other classes or staff in the school. The class teacher monitors the pupil's use of this email address. Pupils are taught that emails sent from their class should have a clear learning purpose and be written in a polite style which is appropriate to the person that will receive it. **We expect all users to communicate appropriately through email.**

- Some pupils and staff will have their own email accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils or staff at school or at home for school purposes. Pupils are taught that using a personalised email account in school or for school use is not permitted. **We expect pupils and staff to use school issued email accounts only.**

Digital Images:

- Digital still and video cameras and camera phones are used for recording 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 consent form for images of their children to be used for school purposes. Parents are reminded of this at school events and are asked not to stream images

to public pages on the internet. The headteacher allows use of cameras and phones at school events providing this is adhered to. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website for which parents give consent on joining the school. On the website 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 at their parent's request.**

- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff. Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school. **All users must adhere to the acceptable use policy when using images of the school community.**

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. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission. **We expect all users to respect copyright laws.**

The Learning Platform:

- The content details on the school website will be the school address, email and telephone number. Staff or pupil contact information will not be published.
- The SLT will take overall editorial responsibility and ensure content is accurate and appropriate.
- No content on the Learning Platform Tapestry is accessible without a username and password allocated by the school.
- Staff will monitor usage of the platform to ensure it is used purely for educational purposes.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted.

Data Protection Act:

- The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) and gives you the right to access information held about you or your child by the school. The school has the right to charge an administrative cost for supplying this information. Further information on the Data Protection Act can be obtained from

  https://www.gov.uk/data-protection

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed yearly.

School IT systems will be reviewed regularly and Virus Protection will be updated regularly in accordance with Medway Council guidelines.

Links with other policies

This online safety policy is linked to our:

Child protection policy
Child on child abuse
Behaviour policy
Data protection policy
Complaints procedure
Acceptable use policy