Buckland Primary School

Online Safety Policy

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of school's ICT systems.

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom.
- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by students when they join the school or start Key Stage 2.
- Acceptable use agreements to be issued to whole school community annually.
- Acceptable use agreements to be held in student and personnel files.

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our online safety coordinator is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Headteacher.
- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school child protection procedure.

Review and Monitoring

Online safety is integral to other school policies including the ICT and Computing Policy, Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's online safety coordinator is responsible for writing, reviewing and updating the policy. The policy will be reviewed on a two yearly basis or more frequently in response to changing technology and online safety issues in the school.

This policy has been developed in consultation with the school's online safety committee and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

2. Education and Curriculum

Student online safety curriculum

The school has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Agreement signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

Staff and governor training

The school will ensure that:

- Staff are provided with updated information on how the GDPR and Data Protection Act affect the way data is collected and stored at school.
- Staff understand the requirements of the GDPR and Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in school.
- Opportunities to share in their children's online safety learning (e.g. assemblies, performances, presentations from Digital Leaders).
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

3. Conduct and Incident management

Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements they have signed. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school's Misuse Plan. The school actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about students.

4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for different ages / stages and different groups of users – staff / students.
- The school regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach.
- The schools anti-virus system is updated daily and managed centrally on the server. When a laptop is switched on it updates. We use Webroot Antivirus.
- The schools anti-virus system is managed centrally and viewed weekly. Virus notifications are emailed out if a laptop is infected and the user is notified.

Social Media

The school has a Social Media Policy that covers the management of school accounts and set out guidelines for staff personal use of social media.

5. Data

The school has a Data Protection and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer (SIRO); and the storage and access of data. The Data Protection and Handling Policy has been reviewed and updated since the introduction of the EU GDPR and the Data Protection Act (2018).

.

6. Equipment and Digital Content

Use of Mobile Technologies

Personal mobile phones and mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices.

Student Use

Student mobile phones must be turned off / placed on silent and stored out of sight in school. They must remain turned off and out of sight until the end of the day. Mobile phones will not be used during lessons or formal school time unless with consent from a member of staff.

If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Authorised staff can search student's electronic devices if they have good reason to think that the device has been or could be used to cause harm, disrupt teaching or break school rules. Any search will be carried out in line with the school's Search Policy – Electronic Devices.

Staff Use

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team.

Staff should not use their own devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Where staff are required to use a mobile phone for school duties – e.g. in case of emergency during off-site activities, or for contacting students or parents - then a school mobile phone will be provided. In an emergency where staff do not have access to a school device, they should use their own device and hide their own number (by dialling 141 first).

Digital images and video

We will seek permission from parents and carers for the use of digital photographs or video involving their child as part of the Use of Digital and Video Images Agreement when their child joins the school.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.