Hitherfield Primary School and Children's Centre

Whole School
Internet Safety Policy

'Our vision is to create a school community where everyone feels valued, has the opportunity to explore and develop their strengths and is able to participate in new experiences. We aim to become an inspirational school to produce good citizens for the future in an atmosphere that promotes confidence, high academic achievement, physical health and emotional well-being.'

Reviewed	Reviewers	Author	Next review
July 2017	LAPD & GB	Luke Parker	July 2020
Jan 2021	LAPD & GB	Chris A-J	Jan 2023

HITHERFIELD PRIMARY SCHOOL

Internet Safety Policy

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.

Responding to concerns

- The school will take all reasonable precautions to ensure internet 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 school inclusion leader is the first point of contact for any complaint. Any concerns about staff misuse will be referred to the Headteacher.
- Concerns that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Concerns related to child protection are dealt with in line with the school child protection procedure.

HITHERFIELD PRIMARY SCHOOL

1. Education and Curriculum

Student internet safety curriculum

The school has a clear, progressive internet 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 Policy 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 understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on internet safety issues and the school's internet 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.
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

2. Conduct and Incident management

Conduct
All users are responsible for using the school ICT systems in line with the Acceptable Use Policy they have signed. They should understand the consequences of misuse or access to 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 e.g google drive, school blog.

Parents and carers 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 internet safety issues. Parents and carers will be informed of any internet safety incidents relating to their own children.

3. 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 internet 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.
- All users will be provided with a username and secure password. Users will be responsible for the security of their username and password.
- Each class has a group log-on and password.
- The administrator passwords for the school ICT system, used by the Network Manager is also available to the Headteacher and kept in a secure place.
- 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. 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 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.
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

4. 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 Advanced IT Technician; and the storage and access of data.

5. Equipment and Digital Content

Personal mobile phones and mobile devices

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.

HITHERFIELD PRIMARY SCHOOL

Student Use

The school strongly understands that older children may need to bring their mobile phones into school if they are walking to or from school alone.

Student mobile phones must be turned off / placed on silent and stored in the main office 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.

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.

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.

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 without prior permission from the Executive Headteacher or Head of School. This permission would only be granted in exceptional circumstances, such as in an emergency on a school trip or if staff were directed to work from home and asked to contact families. 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).

Mobile phones and other devices will be switched off or switched to 'silent' mode. And only used in the offices and the purple zone during school hours. If a staff member needs to be contacted urgently they should ask the person concerned to contact them via the main school office telephone nukber.

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.

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.

We do not identify pupils in online photographic materials or include the full names of students in the credits of any published school produced video.

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.