GISBURN ROAD C.P. SCHOOL

BARNOLDSWICK

DIGITAL SAFETY POLICY

GISBURN ROAD
COMMUNITY
PRIMARY SCHOOL

DATE AGREED: NOVEMBER 2018

REVIEW DATE: NOVEMBER 2020

Based on guidance from the Lancashire Schools' ICT Centre

Contents

1. Introduction

This policy applies to all members of the Gisburn Road community (including staff, pupils, parents/carers, visitors and school community users).

Our Digital Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

2. Gisburn Road vision for Digital Safety

Our school aims to embrace modern technology to its fullest potential, and promote its safe use by all members of the Gisburn Road community. We want all our children and staff to be confident with a range of technology, using it confidently to meet their needs. However, we believe whole-heartedly that children at Gisburn Road should be educated thoroughly in keeping safe when using ICT, from their very first days at the school. As a result, children will be safe in using technology they may encounter both within, and out of, the school environment. A balance is maintained between the need to learn effectively and the need for effective security measures.
Our children will leave Gisburn Road knowing how to use technology effectively, responsibly and safely, and will be equipped with the skills they will need to be successful in the rest of their lives.

3. The role of the school's Digital Safety Champion

The school's Digital Safety Champion is Nick Browne/Computing Subject Leader.

The role of the Digital Safety Champion in our school includes:
- promoting and monitoring the safe use of ICT within school
- ensuring all children are educated in the safe use of ICT, within and out of the school environment
- monitoring and reviewing the Digital Safety policy, and Acceptable Use Policies
- keeping up-to-date with technological and Digital Safety developments
- training staff members on the safe use of technology as necessary, ensuring all staff are aware of reporting procedures in the event of a Digital Safety incident occurring.
- being the school's point of contact for Digital Safety related issues and incidents
- liaising with the school's DSP where necessary in the case of child protection
- ensuring the Digital Safety Incident Log is appropriately maintained and regularly reviewed
- arranging or providing Digital Safety advice/training for parents/carers/governors as necessary

4. Policies and practices

This section of the Digital Safety Policy sets out the school's approach to Digital Safety along with the various procedures to be followed in the event of an incident.

This Digital Safety policy should be read in conjunction with the following other related policies and documents:
Acceptable Use Policy
Social Media Policy

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

1. The Head teacher has ultimate responsibility for all the information that is held in school, and is in charge of managing all data and information, both within and outside the school environment.
2. Relevant staff will be shown the location of data necessary to their position during the induction process.
3. Staff should only access data with which they are authorised to do in line with their job description.
4. Staff with access to school data outside of the school environment are made aware of the importance of ensuring the security of the data, for example ensuring laptop computers and wireless networks are password-protected. Further guidance is provided in the Data Protection Policy, and the Staff Handbook. Staff should only access data outside of the school environment where it is necessary to fulfil their job description, and where the school premises are closed.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

1. All devices with 3G/4G wireless connections can access unfiltered internet content. Therefore, this facility must be turned off before children use such devices.
2. Any devices that use the school network must contain up-to-date virus software.
3. Portable USB devices are permitted to be used, as the school has up-to-date Anti-Virus software. However, staff must ensure that personal computers that the devices are also used with have sufficient Anti-Virus protection.
4. Staff are permitted to bring in personal mobile devices, however these must be kept securely. These must only be used appropriately for personal reasons, for example not making or receiving personal phone calls when children are present. Any data captured on such devices for professional reasons, for example a voice recording during a lesson, must be transferred onto a school computer and deleted immediately from the mobile device. It is not acceptable for staff to take pictures on mobile phones.
5. Pupils may on occasion need to bring a mobile phone into school. However, they must leave it at the school office before registration, and may collect it at the end of the day. All staff can confiscate any personal mobile devices that are deemed valuable and desirable, and will arrange for them to be kept securely in the office.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below:

1. All children, on induction to the school, are required to consent to the use of photographs, videos and appearance in local (or national) media. An up-to-date list of permissions is kept in the school office, where staff can access them prior to taking any pictures and videos. A child's parents/carers can change these permissions at any time by notifying the school office, where a new form will need to be completed and signed.

3. Full names or personal details will not be used on any digital media that is published.
4. Parents/Carers are permitted to video or photograph certain school events, such as school productions and assemblies. Parents will be reminded not to share images on social media or video sharing sites. Events may be recorded by the school, or by a private company assigned by the school, and later made available for parents/carers to purchase. Parents/Carers who do not wish their child to be photographed/recorded can express these wishes to the Head teacher or other staff, who will make appropriate arrangements.
5. Staff are required to understand the risks associated with publishing images and the school policy of not publishing an image where it can be linked to the name of a child.
6. Photographs/videos should only be taken using school equipment, for school purposes. This content should only be stored on equipment that is for predominantly school use. Staff should always make sure that children are appropriately dressed and not participating in activities that could be misinterpreted.
7. All staff and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites without the consent of the persons involved. - See the school's Social Media Policy.
8. The guidelines for safe practice and relevant Acceptable Use Policies are monitored every year by the Digital Safety champion, who will liaise with the Headteacher as required.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email:

1. It is recommended that all users have access to the Lancashire Grid for Learning service as the preferred school e-mail system. Any staff wishing to have a school email address should request that one is created by the Head Teacher.
2. The Lancashire Grid for Learning filtering service should reduce the amount of SPAM

(Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
3. All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school. Personal email accounts should not be checked in the presence of children, or connected to the overhead projectors/whiteboards.
4. All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
5**.** All users are aware that all email communications may be monitored at any time.
6. All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
7. Children are not permitted to access personal email accounts in the school environment. For the purpose of teaching 'Electronic Communication' or communicating with other children, for example pen pals, children may use the pupil accounts set up on the lancsngfl service whilst supervised.

Social Media:
The use of social media networks by staff is covered in the school Social Media Policy.

Mobile telephones:
At Gisburn Road, the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:
1. Staff are permitted to bring personal mobile phones into school. However, these must not be used in the presence of children, except when necessary, for example on school trips or in emergencies. These must be kept securely and remain the responsibility of the staff.
2. Pupils may occasionally need to bring a mobile phone to school, however they must leave it at the office at the start of the day and collect it at the end of the day. Staff may confiscate any mobile phones brought into classrooms, where they will be kept securely until the end of the day.
3. During school trips, staff will be required to carry mobile phones. Contact details will be left with the Base Contact.

Websites and Class Blogs
In our school the following statements outline what we consider to be acceptable and unacceptable use of the school website and Class Blogs
1. The school website will be maintained by appropriate staff under the monitoring of the Computing Subject Leader.
2. The website is a fundamental place for communicating Digital Safety messages to pupils and parents/carers, and has a dedicated Online Safety section.
3. All staff are aware of the guidance for the use of digital media and personal information on the website and class blog pages.
5. All materials on the website shall adhere to copyright restrictions.
6. Sensitive documents should only be available in 'read-only' formats, such as PDFs.

4.5 Acceptable Use Policy (AUP)

The staff and visitor Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. See separate Acceptable Use Policy.

4.6 Dealing with incidents

In the event that an Digital Safety incident occurs, that contravenes the Digital Safety Policy or agreed Acceptable Use Policy, it is important the protocol below will be followed. It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged in the incident log.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

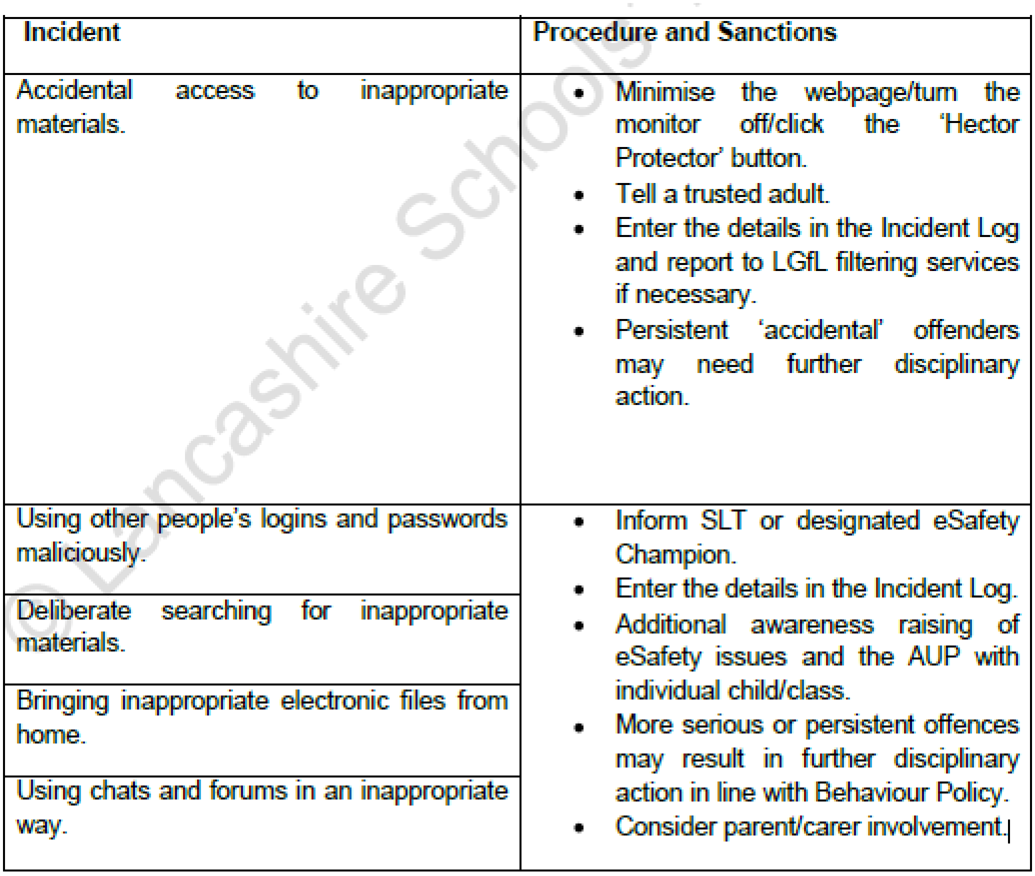
The school will never personally investigate, interfere with or share evidence as this may inadvertently be committing an illegal offence.

The school will always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) as they are licensed to investigate – schools are not.
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk.

Inappropriate use and sanctions
It is important that any incidents are dealt with quickly and actions are proportionate to the offence. If the guidelines or Acceptable Use Policy are breached, or suspected of being breached, the Headteacher should be notified if appropriate. Some examples of inappropriate incidents are listed below with possible sanctions, although this will ultimately be at the discretion of the Headteacher. All incidents should be logged in the Digital Safety incident log.



Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Where staff are suspected of contravening the AUP, this should be reported to the Headteacher who will take appropriate steps in accordance with the school's discipline policy.

Gisburn Road uses a holistic approach to Digital Safety, and as such all staff are responsible for dealing with Digital Safety incidents appropriately at class level. The Digital Safety champion should be notified of any Digital Safety incidents, who will then liaise with the Headteacher as appropriate.

The Digital Safety log book will be kept securely in the Headteacher's office. This will be monitored regularly, with action plans put in place as necessary to avoid further incidents where possible.

The 'Lancashire eSafety Incident/Escalation Procedures' document will be followed as a framework for responding to incidents.

5. Infrastructure and technology

Gisburn Road aims to ensure that our infrastructure and network is as safe and secure as possible. This section of the policy defines the policies and procedures in place to safeguard users.

The ICT network at Gisburn Road is protected by the LGFL/CLEO Broadband filter. However, should unsuitable content not be detected by this filter, children are educated to minimise the screen and inform an adult immediately. Staff will subsequently report the URL of inappropriate content to LGFL/CLEO LightSpeed.

Sophos Anti-Virus is used by the school to protect the network and data from viruses, Trojans and Malware. This is configured by Lancashire to receive regular updates.

6. Education and Training

Education and training are essential components of effective Digital Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Digital Safety is embedded within the curriculum and advantage taken of new opportunities to promote Digital Safety.

6.1 eSafety across the curriculum

Digital Safety is embedded in all areas of the computing curriculum. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology.
Digital Safety rules are displayed wherever computers are used in school. This is differentiated by key stage.

6.2 Digital Safety – Raising staff awareness

All staff, upon starting work at the school, are required to agree to the school's Acceptable Use Policy and are provided with a copy of the Digital Safety policy. Staff training updates for Digital Safety will be delivered as necessary, with a minimum of once per academic year. All training and advice will be delivered by the Computing Subject Leader. The Computing Subject Leader/ Digital Safety Champion is aware of updates to Digital Safety guidelines and receives external training as necessary.
All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting Digital Safety whilst using ICT.

6.3 Digital Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).
Gisburn Road offers regular opportunities for parents/carers and the wider community to be informed about Digital Safety, including the benefits and risks of using various technologies. This takes place through:

- School newsletters
- A dedicated area on the school website, which promotes external Digital Safety resources and online materials
- Parents Digital Safety Awareness sessions and advice available from the Digital Safety champion

6.4eSafety – Raising Governors' awareness

- Governors are kept updated on arising Digital Safety matters through updates by the Head Teacher. Governors also review and agree the Digital Safety policy regularly, following discussion with the Digital Safety Champion.
- The Digital Safety log book is also available to the Governors at any time.

7 Standards and inspection

It is crucial that safeguarding procedures, including ICT, are monitored regularly to ensure that the policy is having the desired effect. It is the overall responsibility of the Digital Safety Champion to ensure that the policy is effective in maintaining the safe use of ICT at Gisburn Road.
The Digital Safety Champion will:
- ensure a log book is in place for Digital Safety incidents, which is monitored constantly and appropriate action taken. Additionally, the incident log will be reviewed at the same time as the Digital Safety Policy, to ensure that any issues are addressed in changes to the policies.
- Any new technologies are risk assessed by the Digital Safety Champion, and Acceptable Use Policies amended/devised if necessary.
- Ensure that staff, parents/carers, pupils and Governors are informed of changes to policy and practice
- Review AUPs at least every 2 years, and more frequently as necessary should matters arise.

Overall, Digital Safety at Gisburn Road is the responsibility of all stakeholders – teachers, support staff, pupils, parents/carers and Governors. It is vital that new technologies are readily embraced, with the appropriate steps taken to ensure that they are always used safely.