Primary Online Safety Framework Document

Banks St Stephen's CE Primary School

Lancashire Schools' ICT Centre

2017

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

Tony Sergeant, Sue Kenny, the teaching staff and Governors of Banks St Stephen's CE Primary School

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: **April 2014**

Reviewed – March 2017

The implementation of this policy will be monitored by **Sally Baines**

This policy will be reviewed as appropriate but at least every two years by The **IT Subject Leader.**

Approved by …… (Headteacher) Date ……

Approved by …… (Governor) Date……

Contents

Developing and Reviewing this Policy 2
Contents 3
1. Introduction 4
2. Your school's vision for Online Safety 4
3. The role of the school's Online Safety Champion 4
4. Policies and practices 5
4.1 Security and data management 5
4.2 Use of mobile devices 6
4.3 Use of digital media 6
4.4 Communication technologies 6
4.5 Acceptable Use Policy (AUP) 9
4.6 Dealing with incidents 9
5. Infrastructure and technology 10
6. Education and Training 11
6.1Online Safety across the curriculum 11
6.2Online Safety – Raising staff awareness 11
6.3Online Safety – Raising parents/carers awareness 12
6.4Online Safety – Raising Governors' awareness 12
7 Standards and inspection 12

Online Safety Policy 2017 Banks St Stephen's CE Primary School

1. Introduction

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

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online 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. Our school's vision for Online Safety

At Banks St Stephen's Primary School we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our Online Safety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view Online Safety education as a key life skill.

Our Online Safety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

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

Our Online Safety Champion is Sally Baines

The role of the Online Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety policy and associated documents, including Acceptable Use Policies
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up to date with Online Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils and Governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person/Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

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.

All data in our school must be kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP).

4.1 Security and data management

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:

- The Online Safety champion and Headteacher are responsible for managing information
- Staff know and are aware of their legal responsibilities

- Staff know that only approved means to access, store and dispose of confidential data are allowed
- Only removable devices issued by the school are allowed to be used on school machines. These are password protected and encrypted.
- The school has backup systems in place to ensure the risk of data loss is addressed and managed.

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:

- Staff need to be aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content.
- All devices need to be virus checked before use on school systems.
- Staff need to consider what wider implications need to be considered for pupils' use of personal mobile devices. Allowing pupils, for example, to bring mobile phones into school also raises the issue of having valuable and desirable personal equipment on the premises.

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.

- As a school we will seek consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used.
- We will seek permission at the beginning of the school year or when a pupil or member of staff starts.
- We will only retain images of pupils after they have left our school for records of achievement and if they are included on a current school prospectus. This time period been made explicit to parents/carers.
- Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs, and are made aware of any conditions in advance.
- Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- All staff are aware that photographs/videos are only taken using school equipment and only for school purposes.
- Our school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- We do not allow staff to store digital content on personal equipment.
- When taking photographs/video, all staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved. This is achieved through PSHE lessons, staff review and training and information evenings, newsletters and advice guides.

4.4 Communication technologies

At Banks St Stephen's we use a variety of communication technologies and we are aware of the benefits and associated risks. The following are examples of technologies that we regularly use in school and how we expect them to be used and managed.

Email:

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

- All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
- 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.
- 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.
- 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.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

When sending emails in school the following standard disclaimer should be included at the bottom of all outgoing emails

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Banks St Stephen's Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:

Many adults and pupils regularly use Social Network sites, e.g. Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Pupils must not be added as friends on any Social Network site.
- Whatever means of communication staff use they should always conduct themselves in a professional manner.

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

At Banks St Stephen's we allow staff and visitors to use their phone during the school day on the condition that it does not impact on working hours i.e. teaching time. Personal mobile phones must be switched off or kept on silent mode during normal school hours unless by prior arrangement with the Headteacher for emergency purposes. Personal mobile phones may be used for emergencies on school trips although the school does provide a school mobile which is preferred.

At no point should the phone be used to capture photographs or other personal data, or for use of the internet including social networks.

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

Instant Messaging, e.g. Skype, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' these sites by default, but access permissions can be changed at the request of the Headteacher

At present we have no plans to 'unblock' these sites. A system is set up for secure messaging, forum and chat systems within their Virtual learning Environment - Moodle.

Virtual Learning Environment (VLE) / Learning Platform:

The children and staff at Banks St Stephens have access to and personal logins for web based learning platforms such as My Maths and Purple Mash. These learning environments allow teachers to set children online activities for completion either in school or at home. The IT coordinator will continue to investigate and evaluate potential Virtual Learning Platforms that mirror or improve upon the now redundant Moodle VLE that was used in school previously.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

Our School website is effective in communicating Online Safety messages to parents/carers. Everybody in the school is made aware of the guidance for the use of digital media and the guidance regarding personal information on the website. The website administrator has access to edit the school website and is responsible for ensuring that this information is current. The Headteacher, Online Safety champion and website administrator have overall responsibility for what appears on the website and that content is subject to copyright/personal intellectual copyright restrictions.

The Online Safety Champion is responsible for monitoring what appears on other sites such as the school's Facebook and Twitter feeds.

Others:

The school will continue to monitor the development of other technologies as and when we consider that they become appropriate for use in our school.

4.5 Acceptable Use Policy (AUP)

At Banks St Stephen's we have a number of Acceptable Use Policies (AUPs) to ensure that all users stay safe whilst using the internet and other communication technologies. These policies reflect the technologies, procedures and practice within our school. All staff and pupils are made aware of these policies and Rules for Responsible Internet Use are displayed in each classroom. These policies are regularly updated. All users are asked to sign an Acceptable Use Policy agreement.

4.6 Dealing with incidents

At Banks St Stephen's we take any incident seriously and have a number of different ways of dealing with them depending on the severity or nature of the incident. Incidents are logged and these are regularly monitored and audited by the Online Safety Champion and if necessary other key members of staff involved in Child Protection. It is likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

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 peoples logins and passwords maliciously.	• Inform SLT or designated Online Safety Champion. • Enter the details in the Incident Log. • Additional awareness raising of Online Safety 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.	

Illegal offences

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

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk). 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

5. Infrastructure and technology

We are fortunate to have excellent facilities for ICT at Banks St Stephen's. They range from portable netbooks and Ipads to fixed desktop machines and classroom teaching laptops. We can facilitate wireless technologies which enables us to use different devices at different times in different locations. We aim to make the infrastructure/network as safe and secure as possible by using the following measures:

- We subscribe to Lancashire grid for Learning/CLEO Broadband Service which provides us with a high level filtering service (Lightspeed) and Sophos Anti-Virus software.
- Pupils have a class login, individual logins in years 5 and 6, to access netbooks and desktops, and these are monitored by the class teacher and ICT Subject Leader/ESafety Champion. Children are supervised when using the equipment.
- Staff have their own logins which are password protected. This is monitored by the Online Safety Champion.
- Pupils have their own login and passwords for Moodle and a Maths site called mymaths.co.uk. This is monitored by the class teacher, Online Safety Champion and Moodle Administrator. They are taught the importance of keeping their password secret and are taught what could happen if it is shared.
- Only approved devices are allowed to use the wireless system. The network key is known by the Online Safety Champion/ICT Subject Leader.
- Only approved and encrypted pen drives can be used on the school's network.
- Our network and infrastructure is supported and maintained by Western Systems
- All software is legally owned with licences provided.

6. Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The three main areas of ESafety risk that our school needs to be aware of and consider are:

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	• Advertising e.g. SPAM • Privacy of information (data protection, identity fraud, scams, phishing) • Invasive software e.g. Virus", Trojans, Spyware • Premium Rate services • Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	• Illegal materials • Inaccurate/bias materials • Inappropriate materials • Copyright and plagiarism • User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyberbullying • Contact Inappropriate emails/instant messaging/blogging • Encouraging inappropriate contact

6.1 Online Safety across the curriculum

It is vital that our pupils are taught how to take a responsible approach to their own Online Safety. Our school needs to provide suitable Online Safety education to all pupils and consider the following points:

- We must provide regular, planned ESafety teaching within a range of curriculum areas.
- We must have an additional focus on ESafety during the National Online Safety Awareness Week.
- Online Safety education will be differentiated for pupils with special educational needs
- Pupils are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications
- Pupils are made aware of the impact of Cyberbullying/Sexting and how to seek help if they are affected by these issues, e.g. telling a member of staff or using the worry boxes?
- Pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, e safety rules

6.2 Online Safety – Raising staff awareness

To support our staff, Online Safety training, led by the Online Safety Champion will be delivered on the first INSET of each new school year. This will provide necessary updates or changes to the system, inform and remind staff of best practice and guidelines that we should follow. It is the Online Safety Champion's responsibility to pass on any information related to training or developments in Online Safety.

Further guidance and general Online Safety issues are discussed in staff meetings and through other areas such as Child Protection/Safeguarding training and refreshers. This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy.

6.3 Online 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).

At Banks St Stephen's we strive to work with our parents/carers to inform them about Online Safety and the benefits and risks of using various technologies. This is achieved through School newsletters, our school website and promotion of external Online Safety resources/online materials.

6.4 Online Safety – Raising Governors' awareness

At Banks St Stephen's we believe it is important that Governors, particularly those with specific responsibilities for Online Safety, ICT or child protection, are kept up to date. This is achieved through discussion at Governor meetings, attendance at Local Authority Training, participation in online training through GEL, CEOP or internal staff/governor/parent meetings.

The Online Safety Policy is reviewed and approved by the governing body at least annually. This policy was last reviewed following the completion of the Online Safety Governor Checklist provided by LSCB in March 2017.

7 Standards and inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.

We will know if our policy is having the desired effect as staff and pupils are aware and follow the good practices outlined in this policy, incident logs are reviewed, audited and when necessary followed up with appropriate action.

Changes to the whole or any part of the policy will be reviewed, made and shared with pupils, staff, Governors and parents. The policy can be obtained through our school website or on request from the school office.

Reviewed November 2017 by SLT