Primary ESafety Framework Document

Banks St Stephen's CE Primary School

Lancashire Schools' ICT Centre

2014

Developing and Reviewing this Policy

This ESafety 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 **Tony Sergeant**

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

ESafety 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 ESafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our ESafety 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 ESafety

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 ESafety 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 ESafety education as a key life skill.

Our ESafety 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 ESafety Champion

Our ESafety Champion is Tony Sergeant

The role of the ESafety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's ESafety 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 ESafety incident occur.
- Ensuring the ESafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up to date with ESafety 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 ESafety 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 ESafety 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 ESafety 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. See Appendix 1 & 2.
- 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. See Appendix 3
- 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 ESafety 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, ESafety 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 E 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. See Appendix 4 – 9.

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 (See Appendix 11 & 12) and these are regularly monitored and audited by the ESafety 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 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.	

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 ESafety 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, ESafety 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 ESafety 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 ESafety across the curriculum

It is vital that our pupils are taught how to take a responsible approach to their own ESafety. Our school needs to provide suitable ESafety 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 ESafety Awareness Week.
- ESafety 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 ESafety – Raising staff awareness

To support our staff, ESafety training, led by the ESafety 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 ESafety

Champion's responsibility to pass on any information related to training or developments in ESafety.

Further guidance and general ESafety 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 ESafety – 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 ESafety and the benefits and risks of using various technologies. This is achieved through School newsletters, our school website and promotion of external ESafety resources/online materials.

6.4 ESafety – Raising Governors' awareness

At Banks St Stephen's we believe it is important that Governors, particularly those with specific responsibilities for ESafety, 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 ESafety 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 March 2017 by Governors

APPENDIX 1
Example of Image Consent Letter to Parents

<Insert School's Letterhead>

Dear Parent / Carer
We regularly take photographs/videos of children at our school and believe that these can provide a
valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website/VLE, or in school displays, including digital photo frames.

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as
possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely,

Headteacher

APPENDIX 2
Image Consent Form

Name of the child's parent/carer:.....

Name of child:.....

Year group:.....

Please read the Conditions of Use on the back of this form then answer questions 1-4 below.
The completed form (one for each child) should be returned to school as soon as possible.
(Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school? Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events? Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school? Yes / No

4. May we use your child's image on our school's online publications e.g. website / blog / VLE? Yes / No

5. May we record your child on video? Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event? Yes / No

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: .....

Name (PRINT): .....

Date: .....

Conditions of Use

1. This form is valid whilst your child attends this school or until you inform us otherwise.
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:
1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in
the caption for the picture (possible exceptions to this are large group or team photographs).
3. It is possible that the newspaper will re-publish the story on their website or distribute it
more widely to other newspapers or media organisations.

APPENDIX 3
Example Consent Form for Images to be Taken e.g.at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school production/event name on <*insert date/s>.* We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images/video being used in general circumstances.

Many parents / carers like to take photographs/videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images/videos to be taken by a third party (i.e. other parents). We need to have permission from all parents/carers of children involved in the production to ensure that they are happy for group images/videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images/videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents/carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.
These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,

Headteacher.

****

Child's name: _____ Date: _____

I agree / do not agree to photographs / videos being taken by third parties at the *<insert event> on <Insert date /s>.*

Signed _____ *(Parent / Carer)*

Print name _____

APPENDIX 4
ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of the Headteacher.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name .....
(PRINT)

Position/Role .....

APPENDIX 5
Example of ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.
1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name ..... (PRINT)

Position/Role .....

Appendix 6
Example of ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

☐ I will only use ICT in school for school purposes.

☐ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.

☐ I will only use the Internet and/or online tools when a trusted adult is present.

☐ I will only use my class e-mail address or my own school email address when emailing.

☐ I will not deliberately look for, save or send anything that could be unpleasant or nasty.

☐ I will not deliberately bring in inappropriate electronic materials from home.

☐ I will not deliberately look for, or access inappropriate websites.

☐ If I accidentally find anything inappropriate I will tell my teacher immediately.

☐ I will only communicate online with people a trusted adult has approved.

☐ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

☐ I will not give out my own, or others', details such as names, phone numbers or home addresses.

☐ I will not tell other people my ICT passwords.

☐ I will not arrange to meet anyone that I have met online.

☐ I will only open/delete my own files.

☐ I will not attempt to download or install anything on to the school network without permission.

☐ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

☐ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

☐ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

.....**Parent/Carer Signature**

We have discussed this Acceptable Use Policy and
..... [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at Banks St Stephen's CE Primary School.

Parent /Carer Name (Print) .....

Parent /Carer (Signature) .....

Class .....

Date.....

This AUP must be signed and returned before any access to school systems is allowed.

APPENDIX 7

ICT Acceptable Use Policy (AUP) – Example Parent's Letter

<Insert School's Letterhead>

Dear Parent/Carer,
The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and/or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing eSafety as part of your child's learning, we will also be holding Parental eSafety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about eSafety for parents and carers, please visit the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mrs Kenny, Mr Sergeant or Mrs Tennant.
Yours sincerely

Headteacher

APPENDIX 8
Example of Typical Classroom eSafety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

APPENDIX 9
Example of Typical Classroom eSafety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

APPENDIX 10
Example of Letter to Parents Regarding Parental eSafety Awareness Session

<Insert School's Letterhead>

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted increasingly view Parental eSafety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date:.....Time:.....
...

The session will include reference to the following areas with time for you to ask questions:

☐ What are our children doing online and are they safe?

☐ Do they know what to do if they come across something suspicious?

☐ Are they accessing age-appropriate content?

☐ How can I help my child stay safe online?

The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' ICT Team will address the issues mentioned above.
Yours sincerely

The Headteacher

I / we will be attending the above Parental eSafety Awareness Session

Name(s):.....

Parent / Carer of:..... *Year Group.....*