St Saviour's
Community Primary School

Online Safety Policy

(Including the Acceptable Use Policy)

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

Vision for Online Safety

Our online safety vision statement:

> "To equip children with the skills and knowledge they need to use technology safely and responsibly at the school, in the home and beyond."

Our school provides a diverse, balanced and relevant approach to the use of technology where all children are encouraged to maximise the benefits and opportunities that the technology has to offer. Children will learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Following the school's online safety curriculum the children will be equipped with the skills and knowledge to use technology appropriately and responsibly. The school's online safety curriculum will teach children how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.

The Role of the School's Online Safety Coordinator

Our Online Safety Co-ordinator is Mrs Wood (Deputy Headteacher)

The role of the Online Safety Co-ordinator in our school includes:

- Operational responsibility for ensuring the development, maintenance and review of the 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 the Child Exploitation and Online Protection Centre (CEOP).

- Providing or arranging online safety advice / training for staff, parents / carers and governors.

Security and Data Management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The *Lancashire ICT Security Framework* (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of the General Data Protection Act (2018) (GDPR), 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.

Use of Mobile Devices (including phones)

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:

- The school allows staff to bring in personal mobile phones and devices for their own use. Staff mobile phones can only be accessed in the staffroom and never while children are present. Under no circumstances does the school allow a member of staff to contact a pupil or parent / carer using their personal device.

- Pupils are allowed to bring personal mobile devices / phones to school but they must be handed in to the office and kept in a safe and secure place. Mobile phones must not be used for personal purposes within lesson time. At all times the device must be switched onto silent.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

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 follow the school's guidance below.

- A consent letter is sent to parents / carers as they start school to obtain permission when using images or names in different school media.

- Images of pupils are removed a year after the child has left the school.

- Full names and personal details will not be used on any digital media, particularly in association with photographs.

- Parents / carers cannot take videos and photographs during school performances, assemblies and sports days etc. (Please see Safeguarding and Child Protection Policy)

- Staff, parents / carers recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites (See section on Social Network sites)

- Photographs / videos are only taken using school equipment and only for school purposes.

- Photographs / videos are only accessible to the appropriate staff / pupils.

- When taking photographs / video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.

Communication Technologies

Email:
The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette, 'netiquette'. In order to meet age related expectations in KS1 and KS2, pupils must have experienced sending and receiving emails.

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

Managing Email

- The school gives all staff their own email account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - Staff must inform (the Online Safety Co-ordinator/ line manager) if they receive an offensive email.
  - However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.
  - Incoming email should be treated as suspicious and attachments not opened unless the author is known.
  - School email is not to be used for personal advertising.
  - Check your email regularly.
  - Never open attachments from an untrusted source; consult your network manager first.
  - Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

Pupil Email Accounts

- Pupils are introduced to email as part of the Computing Scheme of Work.
- Pupils may only use approved email accounts on the school system.
- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher / trusted adult if they receive an offensive email.
- The forwarding of chain letters is not permitted.

Social Networking Sites

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

Examples of social networks may include: the Reading Cloud, blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

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

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messaging (IM) and email addresses, full names of friends / family, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the pupil or his / her location.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be taught about how to keep personal information safe when using online services. Each Key Stage will have specific computing lessons dedicated to online safety. This will be further emphasised in main assemblies and during Online safety week each year.
- The school will conduct regular pupil surveys about home use of computing. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.

- The use of online chat is not permitted in school, other than as part of its online learning environment e.g. within the Reading Cloud.
- The use of inappropriate text, images and videos about other pupils or staff is unacceptable and will always be fully investigated once discovered.

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. MSN, 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.

- Staff and children are made aware of the risks involved using this technology e.g. viewing
  inappropriate images or making unsuitable contacts during online safety lessons.
- They will be allowed to use the secure messaging, forum or chat systems within their VLE (e.g. Reading Cloud).

Use of Internet Websites 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:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience in the Reading Cloud.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an acceptable use of school computing resources form before being allowed to access the Internet from the school site.

School Website

- The school website will contain a page outlining the school's online safety messages so that children can use this information when online and outside of the school environment.
- Staff are aware of the guidance associated with the use of digital media and personal information on the school website and this is included in the Acceptable Use Policy.
- Staff or pupil personal contact information will not generally be published. The contact details given online should be that of the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that their image cannot be misused. Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained when they start school before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Video conferencing:

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

- A permissions letter will be made available for parents/carers to sign giving permission for their child/children to participate in video and photographs.
- Approval by the Headteacher will be obtained in advance of the video conference taking place. All sessions will be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment will be supervised at all times.
- All staff supervising video conferencing equipment will know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Whisper Button:

Our Online Safety Council, along with our Parent Council, have helped to develop our school 'Whisper Button'. The button ('Report an Issue') is a way for you to report any online concerns or problems to school so we can help you sort them. If you want to report anything which you feel maybe wrong, please click the link above and complete the online form that will pop up. If you have any questions about the button, please speak to a member of staff in school.

All children in school have been shown the Whisper Button and how to use the resource.

Others:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team is aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

Acceptable Use Policy (AUP)

All staff, pupils, parents / carers will sign an 'Acceptable Use Policy' to make sure that everyone is using the Internet safely.

See appendix for copies of AUPs

Dealing with incidents

Illegal offences
Any suspected illegal material or activity will be brought to the immediate attention of the Headteacher who will refer this to external authorities, e.g. Police, CEOP

Inappropriate use
The school will deal with incidents that involve inappropriate use (see table below). Incidents will be dealt with quickly and actions will be proportionate to the offence. The correct procedures will be followed when preserving evidence to protect those investigating the incident

Incident Procedure and Sanctions

• Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off. • 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. • Deliberate searching for inappropriate materials. • Bringing inappropriate electronic files from home.	• Inform SLT or designated Online Safety Co-ordinator. • Enter the details in the Incident Log. • Additional awareness raising of online safety issues and the AUP with individual child/class.

• Using chats and forums in an inappropriate way.	• More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.

- The Online Safety Co-ordinator will be responsible for dealing with online safety incidents.
- All staff are aware of the different types of online safety incidents, e.g. illegal or inappropriate, and how to respond appropriately.
- Procedures are in place, in the way of an incident log book, which all staff understand how and when to complete. Children are informed of these procedures during online safety lessons.
- Incidents are monitored on a weekly basis by the Online Safety Co-ordinator.
- Measures are in place to respond to and prevent recurrence of incidents.
- Parents or external agencies will be involved as set out in incident report form.

Infrastructure and Technology

Passwords:

- All staff and pupil users may only access the school's networks through a properly enforced password protection policy.
- All users of the school network have a secure username and password.
- The Headteacher and CC Communications technician know the administrator password for the school network.
- All staff and pupils will be reminded of the importance of keeping passwords secure.
- There is an agreed format for creating passwords e.g. mixture of letters, numbers and symbols.

Software / hardware:

- All school software is legally registered and owned by school.
- The nominated online safety representative will have an up to date record of all appropriate licenses for all software.
- All equipment is regularly audited.
- The nominated online safety representative will control and monitor what software will be installed onto the school system.

Managing the network and technical support:

We employ a firm, CC Communications, who manage our school network and provides us with technical support.

Filtering and virus protection:

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the computing subject leader.
- St Saviour's Community Primary School will ensure that the infrastructure / network is as safe and secure as possible.
- St Saviour's Community Primary School subscribes to the Lancashire Grid for Learning / CLEO Broadband Service, Internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.
- Sophos Anti-Virus software is included in the school's subscription, and this is

installed on all school computers as well as staff laptops and set to receive regular updates.
- School ICT systems security will be reviewed regularly.
- Security strategies will be discussed with the Local Authority as needed.

Education and Training

Online Safety Across the Curriculum

- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in online safety will be developed, and online safety will be embedded within the computing scheme of work and the Personal, Social and Health Education (PSHE) curriculum.

Online Safety – Whisper Button

Our Online Safety Council, along with our Parent Council, have helped to develop our school 'Whisper Button'. The button ('Report an Issue') is a way for you to report any online concerns or problems to school so we can help you sort them. If you want to report anything which you feel maybe wrong, please click the link above and complete the online form that will pop up. If you have any questions about the button, please speak to a member of staff in school.

All children in school have been shown the Whisper Button and how to use the resource.

Online Safety – Online Safety Council

- One child from each year group will represent the Online Safety council for the academic year. Our head boy and head girl will also represent the council.
- One member of staff, and a lead link governor will work alongside the Online Safety Council.
- Minutes of the meetings will be taken and shared with the group, and on our school website.
- The Council meet on a termly basis, or more if required.

Online Safety – Raising Staff Awareness

- All staff will be given the school Online Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will use search engines appropriately when accessing the web with pupils.

Online Safety – Raising Parents / Carers Awareness

- Parents and carers attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school website.
- Parents are invited to a yearly update on online safety focusing on how to keep children safe online in the home environment.
- The school will maintain a list of online safety resources for parents/carers.
- The school will ask all new parents to sign the parent / pupil agreement when they register their child with the school.

Online Safety – Raising Governors' Awareness

Governors, particularly those with specific responsibilities for online safety, computing or child protection, will be kept up to date through discussion at Governors meetings and internal staff or parents meetings. They will be made aware of CEOP and of the website ' thinkuknow.co.uk'

Policies and Practices

This policy should be read and implemented in conjunction with whole school policies, including:

- Safeguarding and Child Protection
- Anti-Bullying Policy
- Code of Conduct
- Policy on the Use of Social Networking Sites and Other Forms of Social Media
- Behaviour & Discipline Policy

Monitoring and Review

The Online Safety Co-ordinator monitors the effectiveness of this policy on a regular basis, reporting to the governing body on the effectiveness of the policy and, if necessary, make recommendations for further improvements.

The school keeps an incident log, which is kept in the online safety folder on the school network accessed only by staff. It is the responsibility of the teacher to record incidents in this log. Incidents will be reviewed weekly to check for any recurring patterns. Any patterns found will be addressed appropriately depending on the incident. This could include working with a specific group, class assemblies and / or reminders for parents. Practice and policy will be adapted or changed if the monitoring and reporting of incidents indicates changes need to be made.

Deanne Marsh - 6th June 2016
To be reviewed annually
Updated 1st September 2016

Reviewed – 19th September 2017
Michelle Wood – 19th September 2017
To be reviewed annually

Reviewed – 1st September 2018
Michelle Wood – 1st September 2018
To be reviewed annually.

Reviewed – 14th February 2019
Michelle Wood – 14th February 2019
To be reviewed annually.

Reviewed – 3rd February 2020
Michelle Wood – 3rd February 2020
To be reviewed annually.

Appendix 1

Internet use - Possible teaching and learning activities Activities	Key online safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Lancashire Grid for Learning The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via email or blogs.	Pupils should only use approved email accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail Lancashire Grid for Learning Cluster Microsite blogs
Publishing pupils work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils full names and other personal information should be omitted. Pupils work should only be published on moderated sites and by the school administrator.	Making the News SuperClubs Plus Headline History Lancashire Grid for Learning Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe
http://www.bbc.co.uk/cbbc/curations/stay-safe

Child Exploitation and Online Protection Centre
https://www.ceop.police.uk

Childnet
http://www.childnet.com

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Think U Know
https://www.thinkuknow.co.uk/Teachers/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents / guardians

BBC Webwise is part of the BBC website with help & support for all aspects of internet safety.
http://www.bbc.co.uk/webwise/guides/parents-film

Avoiding Ratting - Remote Access Trojans - https://www.getsafeonline.org/protecting-yourself/avoiding-ratting/

Keeping Young Children Safe Online (UK Safer Internet Centre) - A useful eSafety Guide for parents http://www.saferinternet.org.uk/ufiles/Keeping-Young-Children-Safe-Online.pdf

The Digizen website - "This provides information for educators, parents, carers, and young people. It is used to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible Digital Citizens."
http://www.digizen.org/

'The Parents' and Carers' Guide to the Internet', has been created by CEOP to provide a light hearted and realistic look at what it takes to be a better online parent.
https://www.thinkuknow.co.uk/parents/parentsguide/

A guide from Google to show parents how they can protect your family online.
http://www.google.co.uk/goodtoknow/familysafety/

YouTube Safety Centre - http://www.youtube.com/yt/policyandsafety/safety.html

The 'Digital Parenting Guide' from Vodaphone "Read about the very latest technology and challenges in our new magazine - our Expert View articles, 'How to' guides and Take Action checklists will help you to stay up-to-date and feel more confident about getting involved."
http://www.vodafone.com/content/index/parents/about_digital_parenting/Resources.html

"The Parents Guide to Technology from the UK Safer Internet Centre has been created to answer these questions and introduce some of the most popular devices, highlighting the safety tools available and empowering parents with the knowledge they need to support their children to use these technologies safely and responsibly".
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parents-guide-to-technology

The Cybersmile Foundation website (The Cyberbullying Charity) http://www.cybersmile.org

How to set up the parental controls offered by your internet provider (UK Safer Internet Centre)
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

The parents section of the Know IT All website. The site contains information about positive ways young people are using different technologies, what the risks are to users and it outlines practical advice in avoiding or minimising risks when using online and mobile technologies.
http://www.childnet.com/kia/parents/

Webcam safety- BBC Webwise - http://www.bbc.co.uk/webwise/0/25812110

Child Safety Online Overview (Knowthenet)
http://www.knowthenet.org.uk/knowledge-centre/child-safety

Advice for parents and carers on cyberbullying
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375420/Advice_for_Parents_on_Cyberbullying_131114.pdf

A Parents' Guide to Instagram
http://dwn5wtkv5mp2x.cloudfront.net/downloads/A_Parents_Guide_to_Instagram.pdf

Cyber Streetwise - "Find out about easy steps you can take to protect your home or business from cyber crime" - https://www.cyberstreetwise.com/

APPENDIX 4 – EYFS Pupil User Agreement

St Saviour's
Community Primary School

ICT Acceptable Use Policy (AUP) for EYFS Children

These rules reflect the content of our school's Online Safety 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 computing 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 computing 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 computing 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 computing because I know that these rules are to keep me safe.
- ✓ I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.
- ✓ 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 (AUP) and .... [Print child's name] agrees to follow the online safety rules and to support the safe use of ICT at St. Saviour's Community 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 5 – KS1 / KS2 Pupil User Agreement

St Saviour's
Community Primary School

Pupil Responsible Use of ICT, Internet and Email

We use the school computers and internet connection for learning. These rules will help us to be fair and keep everyone safe.

- ✓ I will ask permission before accessing any websites, unless my teacher has already given permission.
- ✓ I will not look at, change or delete other people's files.
- ✓ I will not bring CDs or flash drives to use in school without permission.
- ✓ I will only use the computers for schoolwork and homework.
- ✓ I will only e-mail people I know, or my teacher has approved.
- ✓ The messages I send will be polite and sensible.
- ✓ When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone.
- ✓ I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- ✓ I will not use internet chat rooms.
- ✓ If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- ✓ I know that the school may check my computer files and may monitor the internet sites I visit.
- ✓ I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

Pupil Agreement

I have read (listened to) and understood the school rules for the Responsible Use of ICT, Internet and Email. I will use the computer system and internet in a responsible way and obey these rules at all times.

Pupil ___________________________ Date of Birth _________

Signed:

__________________________ Date: __________________ Year 1

__________________________ Date: __________________ Year 2

__________________________ Date: __________________ Year 3

__________________________ Date: __________________ Year 4

__________________________ Date: __________________ Year 5

__________________________ Date: __________________ Year 6

APPENDIX 6 – Parent / Carer Consent Form

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 and iPads 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 by …………………………………….. . 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,

Mrs D.M Marsh

Headteacher

St Saviour's
Community Primary School

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 the questions below. The completed form (one for each child) should be returned to school as soon as possible.

(Please Circle your response)

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

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

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

May we record your child on video / Ipad / Ipod? Yes / No

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 for this academic year (2019 / 20)
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. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
8. 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 7 – ICT ACCEPTABLE USE POLICY – STAFF and GOVERNORS

ICT Acceptable Use Policy (AUP)

Staff and Governor Agreement

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 online safety 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, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms. I will not add pupils or family members of pupils as 'friends' on any social network site.

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 pupils 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 Computing Subject Leader / Headteacher.

10. I will ensure that personal data (including data held on SIMs systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy (see Safeguarding and Child Protection 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 report any known misuses of technology, including the unacceptable behaviours of others.

13. 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.

14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. 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.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. 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.

18. I will take responsibility for reading and upholding the standards laid out in the AUP.

I will support and promote the school’s Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

19. 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 computing code of conduct, alongside the schools Code of Conduct and Policy on the Use of Social Networking Sites and Other Forms of Social Media, to support the safe use of ICT throughout the school.

Signature ……………………….………………………………… Date …..…………………

Full Name ……………………..……………………………………………… (PRINT)

Position / Role ………………………………………………………………………………

Accepted for School by ……………………………………………………………..

APPENDIX 8 - ICT ACCEPTABLE USE POLICY – SUPPLY TEACHERS AND VISITORS/GUEST AGREEMENT

St Saviour's
Community Primary School

ICT Acceptable Use Policy (AUP)

Supply Teachers and Visitors / Guests Agreement

For use by any adult working in St. Saviour's Community Primary 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 respect copyright and intellectual property rights.

4. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy (see Safeguarding and Child Protection 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.

5. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

6. I will not install any hardware or software onto any school system.

7. 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 ……………,,,………………………………………………………..………

Accepted for School by…………………………………………………………………..

APPENDIX 9 – Online Safety Incident Log

All online safety incidents must be recorded by the School Online Safety Co-ordinator or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Cyberbullying should also be recorded on the „Integrated Bullying and Racist Incident Record Form 2‟ available via the Lancashire Schools‟ Portal.

Date / Time of Incident	**Type of Incident**	**Name of pupil/s and staff involved**	**System details**	**Incident details**	**Resulting actions taken and by whom (and signed)**
Example: 01 April 2016 9.50 am	Accessing Inappropriate Website	A N Other (Pupil) A N Staff (Class Teacher)	Class 4 Computer 8	Pupil observed by Class Teacher deliberately attempting to access adult websites.	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.