ALL SAINTS
C.E. Primary School

ONLINE SAFETY

POLICY

Approved: October 2018
Review Date: October 2019

"What you are is God's gift
to you, what you become
is your gift to God"

WHO WILL WRITE AND REVIEW THE POLICY?

The school will appoint an Online Safety Champion from the school's SLT. This may be the Designated Safeguarding Lead or Designated Child Protection Coordinator as the roles overlap.

The Online Safety Champion is Mr. TONY CURRIE.

The role of the Online Safety Champion:

- Having operational responsibility for ensuring the development, maintenance and review of the schools 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
- Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the schools Designated Senior Person / Child Protection Officer to ensure a coordinated approach across relevant safeguarding areas.

Our Online Safety Policy has been written by the school, building on the Lancashire and Kent Online Safety Policies and government guidance. It has been agreed by the Senior Leadership Team and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Parents will be requested to sign an Online Safety /Acceptable Use agreement as part of the Home-School Agreement.

OUR VISION FOR ONLINE SAFETY AND WHY INTERNET USE IS IMPORTANT?

- ALL SAINTS provides a diverse, balanced and relevant approach to the use of technology
- Children are encouraged to maximise the benefits and opportunities that technology has to offer
- ALL SAINTS ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively
- We aim to equip children with the skills and knowledge to use technology appropriately and responsibly
- ALL SAINTS teaches how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- We believe that all users in our school community understand why there is a need for an Online Safety Policy
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Pupils will be safe from radical or extremist material when accessing the Internet in school, in accordance with The Prevent Duty 2015.

HOW DOES INTERNET USE BENEFIT EDUCATION?

- It aids the exchange of curriculum and administration data with LCC and DfE;
- It gives access to world-wide educational resources including museums and art galleries;
- It allows educational and cultural exchanges between pupils world-wide;
- For vocational, social and leisure use in libraries, clubs and at home;
- It gives access to experts in many fields for pupils and staff
- It facilitates professional development for staff through access to national developments, educational materials and effective curriculum practice;
- It allows collaboration across networks of schools, support services and professional associations;
- There is improved access to technical support including remote management of networks and automatic system updates;
- It gives access to learning wherever and whenever convenient.

HOW CAN INTERNET USE ENHANCE LEARNING?

- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

HOW WILL PUPILS LEARN HOW TO EVALUATE INTERNET CONTENT?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

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. All Saints School has used 'The Lancashire ICT Security Framework' (published 2005) 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 Regulations (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must is:

- 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.

HOW WILL INFORMATION SYSTEMS SECURITY BE MAINTAINED?

- Virus protection will be updated regularly. All of the computers in ALL SAINTS have 'Sophos' virus protection which is maintained by IT Services - MGL and BT Lancashire (our technical support teams).
- The security of the school information systems and users will be reviewed regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The MGL Technician will review system capacity regularly.
- The school Internet access will be designed to enhance and extend education.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- There are various levels of passwords for different users.
- Tony Currie, Pamela Lilley and Deborah Roebuck are responsible for managing information
- Staff know the location of data relevant to them
- Staff with access to personal data understand their legal responsibilities with reference to confidentiality, and if they are unsure in a certain area, they know to always be cautious and check with HT before releasing any data.
- All sensitive data is to be stored on the school server in password protected areas.
- Extremely sensitive data is in one place where only two people have security access.
- Staff are aware that they should only use approved means to access, store and dispose of confidential data – pass to HT for digital shredding. Children's work can be deleted using the normal 'windows' method.
- All teachers have remote access to their own school data
- Only school purchased, encrypted removable USB drives can be used in ALL SAINTS.

HOW WILL EMAIL BE MANAGED?

- Pupils may only use approved '.lancs.sch.uk' e-mail accounts.
- Staff should not use school or other email accounts to communicate with pupils.
- Only whole-class or group email addresses will be used in ALL SAINTS for communication outside of the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should not use personal e-mail accounts during school hours or for professional purposes.
- All School emails contain the following disclaimer:

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 All Saints CE 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.'

USE OF DIGITAL MEDIA.

As photographs and video of pupils and staff are regarded as personal data in terms of the GDPR, we obtain written permission for their use from the individual and/or their parents or carers.

- Images of pupils are retained indefinitely after they have left School. This is made explicitly to parents/carers in home school agreement.
- Staff and pupils 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 but they are only for use in their home – they are not to be uploaded onto Social Networking Sites. This is made explicitly to parents/carers in school communications
- All Saints playground and foyer is monitored by CCTV. All school visitors are notified of this via signage. Only the Headteacher and named Parish Council representative have access to the recordings.
- All video conferencing (or similar) sessions are logged including the date, time and the name of the external organisation/ person(s) taking part.
- Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- ALL SAINTS ensures that photographs/videos are only taken using school equipment and only for school purposes
- Staff are allowed to store digital content on personal equipment as long as they understand that the personal equipment must be password protected, and no other users at home are allowed access to the content. Setting up a unique password protected school account on a home PC is allowed.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted
- The publishing of images and videos of pupils or adults on Social Network sites or websites (other than the School website) is strictly prohibited.

HOW WILL PUBLISHED CONTENT BE MANAGED?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT').
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

CAN PUPIL'S IMAGES OR WORK BE PUBLISHED?

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Pupils work can only be published with their permission or their parents/carers.

HOW WILL SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING BE MANAGED?

Primary School Pupils are too young to use most social network spaces. Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Snapchat and Instagram. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users content, send messages and leave comments.

All staff need to be aware of the following points:

1. The content on Social Network sites may be unmediated and inappropriate for certain audiences.
2. If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
3. Adults must not communicate with pupils using any digital technology other than through 'MyMaths' and 'Moodle' and then, the content of the communication needs to be appropriate and free from misinterpretation.
4. The content posted online should not:
   - bring the school into disrepute
   - lead to valid parental complaints
   - be deemed as derogatory towards the school and/or its employees
   - be deemed as derogatory towards pupils and/or parents and carers
   - bring into question their appropriateness to work with children and
   - young people.
5. Adults must not communicate with children using any digital technology where the content of the co mmunication maybe considered inappropriate or misinterpreted.
6. Online communications with parents, past pupils or siblings of pupils, especially if under the age of 18 is <u>discouraged</u>.
7. Children must not be added as 'friends' on any Social Network site.

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- 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, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Staff mobile phones are only allowed to be used at set break times.
- During curriculum teaching time all staff <u>should not</u> have their phone with them.
- Personal mobile phones are to be used for security purposes on school activities e.g. school trips
- VOIP and Instant Messaging, e.g. Text messaging, MSN, Skype, Yahoo Messenger, Facetime 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 some of these sites by default, but access permissions can be changed at the request of the Headteacher.
- Only Skype is allowed for Video Conferencing with other Schools via the Head Teacher's PC. On all other PCs, Skype will be blocked

MOBILE PHONES

- Children are not permitted to have mobile phones in school unless agreed with the Headteacher
- Mobile phones are not allowed in toilets or changing areas
- Mobile phones are only allowed to be used at lunch or break times

- We require mobile phones to be ‘on silent’ during the school day
- Staff and visitors bring in mobile phones at their own risk – they are not insured by school

Images, video or audio must not be recorded on a personal mobile phone without specific authorisation from the headteacher

HOW WILL FILTERING BE MANAGED?

- The school will work with LCC, Becta and the Schools Broadband team to ensure that systems to protect pupils are reviewed and improved. ALL SAINTS is part of the Lancashire Grid for Learning/CLEO Broadband Service and so internet content filtering is provided by default.
- Filtering is provided by ‘Lightspeed’ and is adapted by school to ensure it addresses local issues / trends.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Online Safety Champion.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The Computing Lead receives weekly updates on what the filter has blocked and keeps a monitoring record, focusing on any patterns of misuse. (Accidental or otherwise)

HOW CAN EMERGING TECHNOLOGIES BE MANAGED?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time (as part of the School AUP). The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

HOW SHOULD PERSONAL DATA BE PROTECTED?

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018

HOW WILL INTERNET ACCESS BE AUTHORISED?

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.
- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for pupil access (possibly as part of the Home-School agreement)
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is available).
- The school website effectively communicates Online Safety messages to parents/carers
- All website editors are made aware of the guidance for the use of digital media on the website
- All website editors are aware of the guidance regarding personal information on the website
- Only The HT, School Administrators and the website HLTA have permission to edit the school website
- The HT has overall responsibility for what appears on the website
- Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the schools consent

HOW WILL RISKS BE ASSESSED?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- Neither the school nor LCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

ACCEPTABLE USE POLICY (AUP)

- An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.
- AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed
- A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

Our school AUPS:

- Are understood by the each individual user and relevant to their setting and purpose.
- Are regularly reviewed and updated.
- Are regularly communicated to all users, particularly when changes are made to the Online Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
  - Cyber bullying
  - Accessing unlawful material that promotes extremism or radicalisation in accordance with The Prevent Duty 2015.
  - Inappropriate use of email, communication technologies and Social Network sites and any online content
  - Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. Passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions
- Stress the importance of Online Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

DEALING WITH INCIDENTS

- An incident log is completed to record and monitor offences. This is audited half termly by the Online Safety Champion or other designated member of the Senior Leadership Team.

ILLEGAL OFFENCES

- Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet WatchFoundation (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
    - Accessing material that promotes extremism or radicalisation.
- More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

INAPPROPRIATE USE

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. All incidents are dealt with quickly and actions are proportionate to the offence.

Staff follow the system (See Appendix "Guidelines for Online Safety Incidents) when an incidents occurs

- The Online Safety Champion is responsible for dealing with Online Safety incidents
- All staff are aware of the different types of Online Safety incident and how to respond appropriately e.g. illegal or inappropriate.
- All children are informed of the procedures as a part of their training and in day to day lessons if situations arise
- Incidents are logged in the file in the School Office.
- Online Safety Champion monitors incidents on a half termly basis

HOW IS THE INTERNET USED ACROSS THE COMMUNITY?

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

HOW WILL CYBER BULLYING BE MANAGED?

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of Cyber bullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

HOW WILL LEARNING PLATFORMS AND LEARNING ENVIRONMENTS BE MANAGED?

- SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

INFRASTRUCTURE AND TECHNOLOGY

Pupil access

Children are always supervised by a trusted adult when accessing school equipment and online materials

Passwords

Staff are aware of the following guidelines concerning passwords:

- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data involved, e.g. 'master user' passwords are more critical.
- Users are instructed on appropriate techniques for selecting and setting a new password.
- Passwords should be changed frequently to previously unused passwords. Many systems have the capability to prompt or force the user, periodically, to select a new password. The System Manager should decide on the appropriate duration that users could leave their password unchanged. A typical period is termly
- The interval chosen and the methods by which the password changes will be enforced must be suitably documented for users.
- A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as: -when a password holder leaves the school or is transferred to another post; or when a password may have become known to a person not entitled to know it.
- The need to change one or more passwords will be determined by the risk of the security breach.
- Users must not reveal their password to anyone.
- Users who forget their password must request the System Manager issue a new password.
- Where a password to boot a PC or access an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network.
- All users of the school network have a secure username and password
- The administrator password for the school network is available to the Headteacher and is kept in a secure place
- Staff and pupils are reminded of the importance of keeping passwords secure.
- Staff passwords will be changed each term.
- Staff and pupil passwords are combinations of numbers and letters. Administrator passwords are combinations of numbers, letters and special characters.

Software/hardware

- ALL SAINTS has legal ownership of all software
- ALL SAINTS annually audits equipment and software
- BT Lancashire and MGL controls what software is installed on school systems
- BT Lancashire Services manages the network and technical support for admin, MGL for curriculum.
- Servers, wireless systems and cabling is/are securely located and physical access restricted
- All wireless devices have had their security enabled

- All wireless devices are accessible only through a secure password
- Online Safety Champions responsible for managing the security of your school network
- The safety and security of the school network is reviewed monthly
- School systems kept up to date in terms of security e.g. computers regularly updated with critical software updates/patches -monthly
- Users (staff, pupils, guests) have clearly defined access rights to the school network -they have a username and password and permissions assigned according to role
- Staff and pupils are required to lock or log out of a school system when a computer/digital devices left unattended
- Only Online Safety Champion and BT Lancashire are allowed to download executable files or install software
- Users report any suspicion or evidence of a breach of security to Online Safety Champion
- All internal/external technical support providers are aware of ALL SAINTS requirements / standards regarding Online Safety
- ITCoord is responsible for liaising with/managing the technical support staff

HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use. All pupils and staff are required to read and sign the Online Safety agreement and/or the acceptable use policy. Age appropriate discussions will take place with children before the sign the Online Safety Agreement.
- Online Safety rules will be posted in rooms with Internet access.
- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- Pupil instruction in responsible and safe use should precede Internet access.
- All users will be informed that network and Internet use will be monitored.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

HOW WILL THE POLICY BE DISCUSSED WITH STAFF?

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.

HOW WILL PARENTS' SUPPORT BE ENLISTED?

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats including through a dedicated Parental Awareness Session

EDUCATION AND TRAINING

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond.

They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

APPENDICES

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 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, 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 not search for any material deemed extremism or radicalisation in accordance with The Prevent Duty 2015.
7. I will respect copyright and intellectual property rights.
8. I will ensure that all electronic communications with children and other adults are appropriate.
9. I will not use the school system(s) for personal use during working hours.
10. I will not install any hardware or software without the prior permission of Mr Currie
11. 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.
12. 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.
13. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
14. I will report any known misuses of technology, including the unacceptable behaviours of others.
15. 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.
16. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
17. 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.
18. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
19. 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.

20. 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 children to be safe and responsible in their use of ICT and related technologies.
21. 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 ………

ICT Acceptable Use Policy (AUP)

Visitors, Supply Teachers, Students, Guests

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 access any material deemed extremism or radicalisation.
4. I will not use any external device to access the school's network e.g. pen drive.
5. I will respect copyright and intellectual property rights.
6. 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.
7. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
8. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
9. I will not install any hardware or software onto any school system.
10. 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 ……………………………………………………………………………………………………

ICT Acceptable Use Policy (AUP)

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.

1. I will only use ICT in school for school purposes.
2. I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
3. I will only use the Internet and/or online tools when a trusted adult is present.
4. I will only use my class e-mail address or my own school email address when emailing.
5. I will not deliberately look for, save or send anything that could be unpleasant or nasty.
6. I will not deliberately bring in inappropriate electronic materials from home.
7. I will not deliberately look for, or access inappropriate websites.
8. I will not deliberately look for anything that involves extremist or radical views.
9. If I accidentally find anything inappropriate I will tell my teacher immediately.
10. I will only communicate online with people a trusted adult has approved.
11. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
12. I will not give out my own, or others', details such as names, phone numbers or home addresses.
13. I will not tell other people my ICT passwords.
14. I will not arrange to meet anyone that I have met online.
15. I will only open/delete my own files.
16. I will not attempt to download or install anything on to the school network without permission.
17. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
18. 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 Online Safety .
19. 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.

We have discussed this Acceptable Use Policy.

………………………………………………………… [Print child's name] agrees to follow the Online Safety rules and to support the safe use of ICT at All Saints CE School

Parent /Carer Name (Print) ……………………………………………………………………………………………………

Parent /Carer (Signature) ……………………………………………………………………… …………………………

Class ………………………………………………… Date……………………………………………………………………

ICT Acceptable Use Policy (AUP)

Example Letter

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 Online Safety 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 Online Safety as part of your child's learning, we will also be holding Parental Online Safety 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 Online Safety for parents and carers, please visit the Lancsngfl Online Safety website http://www.lancsngfl.ac.uk/Online Safety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact me.
Yours sincerely,

Mr Currie

Online Safety Golden Rules

1) We always ask permission before using the internet and ensure a trusted adult is near us while we use it.
2) We tell a teacher straight away if we see something we do not like or we think is not appropriate.
3) When we talk to people using computers, we are polite and friendly.
4) We keep information about who we are safe, secret and secure.
5) We will only click on buttons if an adult has said its okay to do so.
6) We will not use any personal devices in school unless approved by a trusted adult.

Online Safety Golden Rules

1) We always ask permission before using the internet and ensure a trusted adult is near us while we use it.
2) We immediately close / minimise any page we feel uncomfortable with and tell

   the responsible adult about it. (Switch off the monitor if necessary)
3) We only communicate with people a trusted adult has approved.
4) All our digital communications are friendly and polite.
5) We keep our personal information safe, secret and secure.
6) We will only use software approved by a trusted adult in school.
7) We will not use any personal devices in school unless approved by a trusted adult.

ICT / Online Safety Training

Example Letter

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 technology 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 inspections increasingly view Parental Online Safety 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 address 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 1.25 hrs where a member of the Local Authority Schools' ICT Team will present an Internet Safety session to address the issues mentioned above.

Yours sincerely,

I / we will be attending the above Parental Online Safety Awareness Session

Name(s): ……………………………………………………………………………………

Parent / Carer of: ………………………………………………………… Year Group ……………………………

ONLINE SAFETY INCIDENT LOG

All Online Safety incidents must be recorded by the School Online Safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Cyber bullying should also be recorded on the Integrated Bullying and Racist Incident Record Form 2 available via the Lancashire School's 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)

GUIDELINES FOR ONLINE SAFETY INCIDENTS

*In the event of any breach of Online Safety Procedure; guidelines for sanctions are outlined below and details of **any** incident is recorded on the Online Safety Incident Log.*

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Online Safety Champion	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg yellow card / red card
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓							✓	✓
Unauthorised use of mobile phone / digital camera / other mobile device	✓					✓		✓	✓
Unauthorised use of social media / messaging apps / personal email	✓	✓				✓		✓	✓
Unauthorised downloading or uploading of files	✓	✓							✓
Allowing others to access school network by sharing username and passwords								✓	
Attempting to access or accessing the school network, using another pupil's account								✓	
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓							✓
Corrupting or destroying the data of other users	✓								✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓			✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓			✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓			✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓						

GUIDELINES FOR ONLINE SAFETY INCIDENTS

*In the event of any breach of Online Safety Procedure; guidelines for sanctions are outlined below and details of **any** incident is recorded on the Online Safety Incident Log.*

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Possible suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				
Inappropriate personal use of the internet / social media / personal email	✓	✓				✓		✓
Unauthorised downloading or uploading of files	✓					✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓					✓		
Careless use of personal data eg holding or transferring data in an insecure manner	✓					✓		
Deliberate actions to breach data protection or network security rules	✓	✓				✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓						✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓					✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils.	✓	✓	✓				✓	✓
Actions which could compromise the staff member's professional standing	✓	✓						✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	✓	✓						✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓				✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓				✓	✓
Breaching copyright or licensing regulations	✓	✓						✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓				✓	✓