Saint Augustine's Catholic Primary School

eSafety and Social Media Policy 2018

Agreed by Governors and staff

December 2014

Review Date

December 2015

List of Appendices

1. Introduction

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

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

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. It should be read in conjunction with the following other related policies and documents:

- Child Protection Policy
- Anti-bullying Policy
- Behaviour Management Policy
- Staff code of Conduct, Recruitment and Induction Procedures

2. St Augustine's school's vision for eSafety

St Augustine's provides a diverse, balanced and relevant approach to the use of technology.

- Through a variety of media the children are encouraged to maximise the benefits and opportunities that technology has to offer.
- The school aims to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.
- The children are increasingly being equipped with the skills and knowledge to use technology appropriately and responsibly.
- The school aims to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.

3. The role of the Senior Leadership Team.

The role of the Senior Leadership Team and eSafety co-ordinator include:

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

4. Policies and Practices

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

4.1 Security and data management

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

This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- All laptops are password protected
- All children have their own password and are encouraged not to share it.
- All data in the school is kept secure and staff informed of what they can or can't do with data through the eSafety Policy and statements in the Acceptable Use Policy (AUP).
- The Senior Leadership Team are responsible for managing information
- Staff are aware of where data is located
- All staff with access to personal data understand their responsibilities.
- The school ensures that data is appropriately managed both within and outside the school environment .
- The staff are aware that they should only use approved means to access, store and dispose of confidential data
- Staff have access to school logins, to ensure the data remains secure.

- The school's policy on using mobile devices and removable media is that school information is not allowed to be carried on pen drives and no school data is allowed to be removed out of school on removable devices unless they are password protected. Staff are responsible for their own pen drives.
- The school aims to ensure that data loss is managed by the use of passwords for the required people.
- The school's procedure for backing up data is on hard drives which are updated on a regular basis with one copy always kept off-site.

  We also have our Data protection Policy 2018 which sets out our compliance with GDPR regulations.

4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, tablets, game consoles or netbooks can access unfiltered internet content.

Pupils:
Mobile phones are not allowed to be brought into school by children. If a phone is brought in by mistake or is needed after school the children are asked to hand the phone into a teacher, which will be taken to the office to be stored securely until the end of the day.

Tablets are allowed to be brought in by Year 6 pupils on our annual Christmas Toy day. Pupils are given the network password to ensure they access appropriate content. We accept no responsibility for these devices in the event of loss and/or damage.

Staff:
The school allows personal mobile phones to be used in school by staff and visitors but are asked to be left on silent in curriculum time. Staff are allowed to use their mobile phones to access schools internet at lunch times. It is acceptable to use personal mobile phones for school activities e.g. school trips for safeguarding reasons. Staff may use their mobile phones to access CPOMS using their two-factor authentication.

Under no circumstances must mobile phones or personal cameras be used to capture images, video or audio.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display as long as parental consent is obtained.

- At school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers.
- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used.
- The parental/carer permission is obtained when they join the school, but the parents have a right to change this if deemed necessary.
- The 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 as long as they are of their own child, for personal use and are reminded that they must not be published on line under any circumstances.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes.

- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff must not store digital content on personal equipment. The staff are not permitted to use their own cameras.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the S.L.T and Governors on an annual basis.

St Augustine's will not pass on any phone numbers or email addresses to third parties.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

- All users have access to Google Mail as the preferred school email system.
- Children are given their own unique email address when they join the school eg j.smith@stuaugstinespreston.co.uk. This email is restricted so emails can only be sent internally eg to other pupils and not outside of school.
- Only official email addresses are used between staff and with other agencies when personal/sensitive data is involved.
- The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

St Augustine's school email disclaimer:

****
This e-mail is confidential and privileged. If you are not the intended recipient do not disclose, copy or distribute information in this e-mail or take any action in reliance on its content.
****
****
This email has been checked for known viruses.

Social Networks:

Social Network sites allow users to be part of a virtual community. 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.

Social networking applications include, but are not limited to:

- Blogs, for example Blogger
- Online discussion forums, such as netmums.com
- Instant messaging such as MSN, Skype and Yahoo Messenger
- Collaborative spaces, such as Facebook, Bebo, My Space, Club Penguin and Google +
- Media sharing services, for example YouTube
- 'Micro-blogging' applications, for example Twitter

Guidance/protection for Pupils on using social networking:

• No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and MSN. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is:
http://www.facebook.com/help/contact.php?show_form=underage
• No school computers are to be used to access social networking sites at any time of day.
• Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision
• Please report any improper contact or cyber bullying to you class teacher in confidence as soon as it happens.
• We have a zero tolerance to cyber bullying

Guidance/protection for Staff on using social networking:

- Information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.
- They must also operate in line with the School's Equality and Diversity Policy. They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Children who are under 13 are not legally allowed to members of Facebook.
- It is illegal for an adult to network, giving their age and status as a child
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection person in school (J.Entwistle)

Staff must not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- put school representatives in breach of school codes of conduct or policies relating to staff;
- be deemed as abusive or hateful in manner;
- lead to valid parental complaints;

- be deemed as derogatory towards the school and/or it's employees;
- be deemed as derogatory towards pupils and/or parents and carers;
- bring into question their appropriateness to work with children and young people.

Staff must also refrain from:

- Discussing any matters relating to school, staff, pupils or parents
- Identifying themselves as a representative of the school
- Adults must not communicate with pupils or ex-pupils using any digital technology (unless it is through the VLE and is conducted from school in school time)
- Referencing should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Adding pupils (or ex-pupils) and parents as 'friends' on any Social Network site. (Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher).

Staff must be aware that violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee, up to and including termination of employment.

Web sites and other online publications:

This may include for example, podcasts, videos, 'Making the News' and blogs.

- The school website is effective in communicating eSafety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media on the website.
- Everybody in the school aware of the guidance regarding personal information on the website.
- Only certain members of staff have access to edit the school website. They have been trained appropriately.
- The Head teacher has overall responsibility for what appears on the website.

Others:

The school will adapt/update the eSafety policy in light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

4.5 Acceptable Use Policy (AUP)

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

AUPs are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school AUPS aim to:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
    - Cyberbullying
    - 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 (linked to our Behaviour Management Policy).
- Stress the importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

This is reviewed yearly.

4.6 Dealing with incidents

At St Augustine's an eSafety Incident Log (see appendix 8) is completed to record and monitor offences. This is stored with the Safeguarding files and is audited on a regular basis by the eSaftey co-ordinator.

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 Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation (http://www.iwf.org.uk) . They are licensed to investigate – schools are not!
Examples of illegal offences are:

- Accessing child sexual abuse images

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

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

Inappropriate use

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied.

Some examples of inappropriate incidents are listed below with suggested sanctions.

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

The SLT is responsible for dealing with eSafety incidents. All staff are aware of the different types of eSafety incident and how to respond appropriately. e.g. illegal or inappropriate. Procedures are in place to deal with eSafety incidents and all staff aware of these.

- Children are informed of the procedures through discussions with members of staff.
- These incidents are logged on the incident log kept in the office. (See Appendix 8)
- Incidents are monitored, by the SLT on a regular basis.
- The measures that are in place to respond to and prevent recurrence of an incident.
- The SLT will decide at which point parents or external agencies are involved
- The procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member (Appendix 9)

The school uses the 'eSafety Incident/ Escalation Procedures' document (See Appendix 9) as a framework for responding to incidents.

5. **Infrastructure and Technology**

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided (by default) by the Lancashire Grid for Learning.

Pupil access:

- The children are supervised by staff when accessing school equipment and online materials

Passwords:

- All staff aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at http://www.lancsngfl.ac.uk/esafety/index.php?category_id=13.
- All users of the school network have a secure username and password.
- The administrator password for the school network available to SLT/ ICT co-ordinator and ICT technicians
- Staff and pupils are reminded of the importance of keeping passwords secure
- Youtube access is password protected and only teaching staff know this password.
- Passwords will only be changed if the need arises.

Software/hardware:

- The school has legal ownership of all software.
- The school has an up to date record of appropriate licences for all software and the Computing co-ordinator is responsible for maintaining this.

Managing the network and technical support:

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT is responsible for managing the security of the school network.
- The safety and security of the school network is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.
- Users report any suspicion or evidence of a breach of security to the SLT
- The school insists staff only use encrypted removable storage devices on school equipment which are not to be used on any unprotected computer

- The school encourages teachers to follow esafety policy guidelines when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with the Data Protection Act (1998)
- All internal/external technical support providers are aware of your schools requirements /standards regarding eSafety
- The SLT is responsible for liaising with/managing the technical support staff.

6. Education and Training

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

The main areas of eSafety risk that we need to consider:

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

6.1 eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. St Augustine's provides suitable eSafety education to all pupils:

- Regular, planned eSafety teaching within a range of curriculum areas
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of computing both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules (See Appendices), acceptance of site policies when logging onto the school network

6.2 eSafety – Raising staff awareness

- The eSafety co-ordinator provides advice/guidance or training to individuals as and when required.
- eSafety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of computing and digital resources.
- eSafety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy.
- Regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

6.3 eSafety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

The school offers opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies. For example through:

- Local Authority eSafety courses run in school
- School newsletters, homework diaries, Website, VLE and other publications.
- Promotion of external eSafety resources/online materials.

6.4 eSafety – Raising Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for eSafety, Computing or child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP (Child Exploitation and Online Protection) and or internal staff/parent meetings.

NB The eSafety Policy will be reviewed yearly (and/or if a serious breach occurs) by the eSafety coordinator, approved by the governing body and made available on the school's website.

7. Standards and Inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.
At St Augustine's:

- E-Safety incidents are monitored, recorded and reviewed.
- The SLT are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is risk assessed.

- These assessments are included in the eSafety Policy.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.
- These patterns would be addressed most effectively by e.g. working with a specific group, class assemblies, reminders for parents.

Cyber-bullying

It is vital that children learn how to be safe when using new technologies of the computer and mobile phone. There needs to be a focus on empowering children by equipping them with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online.

Investigation of alleged cyber-bullying:

Children will be encouraged to do the following if they receive a nasty message:

» Save it (eg screenshot).

» Not to reply.

» Block future messages.

» Show it to their parents or a member of staff.

If the perpetrator is a child who attends this school the parent will be encouraged to report it to a member of staff at school. The member of staff will ensure that the children's class teachers are aware of the investigation. The class teacher will investigate the allegation with the perpetrator and recipient and report to the Assistant Head or Head teacher.

Action:

The Head or Assistant Head will write to the perpetrator's parents and report the nature of the cyber-bullying.

- A first incidence of cyber-bullying will warrant a warning by letter and a Yellow Card in school.
- Any further incidences will warrant further sanctions and parents called in
- Serious and/or persistent cyber-bullying may result in a fixed term seclusion/exclusion and the involvement of the Police.

Appendix 1 –

St Augustine's – Image Consent Form

Name of child:_____

Class:_____

Name of the child's parent/carer: _____

We regularly take photographs/videos of children at our school. The vast majority of these are used for class displays, work evidence, class photographs or for our class year books. Occasionally these may be used in our school brochure, in other printed publications or on our school website.

Also, our school may be visited by the media 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.

In order that we can protect your child's interests, and to comply with the Data Protection Act (1998), **please read the Conditions of Use on the back of this form, then answer questions 1-3 below. Please sign, date and return the completed form (one for each child) to school as soon as possible. (Please Circle)**

I understand that my child's photograph can be used for school purposes such as class displays, work evidence, class photographs or for our class year books unless I write to opt out of this.

1. May we use your child's photograph in printed school publications purposes?.....Yes / No

2. May we use your child's image on our school website? ..... Yes / No

3. 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 the length of time that your child is at St Augustine's Catholic Primary School.
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 pupils, 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 pupils who are suitably dressed.

7. 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 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 2

St Augustine's - ICT Acceptable Use Policy (AUP) Staff and Governor Agreement

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

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not discuss any matters relating to school, staff, pupils or parents on-line
5. I will not identify myself as a representative of the school on-line
6. I will not communicate with pupils or ex-pupils using any digital technology (unless it is through the VLE and is conducted from school in school time)
7. I will not reference any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
8. I will not add pupils (or ex-pupils) and parents as 'friends' on any Social Network site. (Where family and friends have pupils in school and there are legitimate family links, I will inform the head teacher).
9. 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.
10. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
11. I will respect copyright and intellectual property rights.
12. I will ensure that all electronic communications are appropriate.
13. I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)
14. I will not install any hardware or software without the prior permission of the SLT
15. 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.
16. I will ensure that Images of pupils and/or adults will be taken only on school cameras, stored only on school equipment 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.
17. I will report any known misuses of technology, including the unacceptable behaviours of others.
18. 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.
19. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
20. 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.

21. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
22. I am aware that in certain circumstances where unacceptable use is suspected, enhance monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
23. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
24. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

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

Signature ……..…… Date ……..……..……

Full Name ……..……..……
(PRINT)

Position/Role ……..……...…….

Appendix 3 –

St Augustine's - ICT Acceptable Use Policy (AUP) Supply teachers and Visitors/Guests Agreement

For use with 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 communicate with pupils or ex-pupils using any digital technology
3. I will not reference any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
4. I will not add pupils (or ex-pupils) and parents as 'friends' on any Social Network site. (Where family and friends have pupils in school and there are legitimate family links, I will inform the head teacher).
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 Images of pupils and/or adults will be taken only on school cameras, stored only on school equipment 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.
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 ……..……...…….

St. Augustine's Catholic Primary School

St. Austin's Place, Avenham, Preston, PR1 3YJ. Tel: 01772 253851

Headteacher: Mr John Entwistle (BEng(Hons), PGCE, Dip Ed.)

emails: office@st-augustines-pri.lancs.sch.uk, head@st-augustines-pri.lancs.sch.uk

ICT Acceptable Use Policy (AUP) – Parents' Letter

Dear Parent/ Carer,

The use of ICT including the Internet, email, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites such as Facebook do have 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 these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour Management Policy outlines those principles we expect our pupils 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.

If you would like to find out more about eSafety for parents and carers, please visit the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

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

Yours sincerely,

J. Entwistle

Mr J. Entwistle (Headteacher)

Appendix 5

St. Augustine's Catholic Primary School
e-Safety Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil's name:	***Class:***

Pupil's Agreement

- I have read, understand and agree to follow the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I agree that appropriate images and video that include my son/daughter may be published subject to the school "Image Consent Rules".

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to your child's class teacher as soon as possible.

For more information you can see the full school policy and Image Consent rules attached

Appendix 6

Please read all the statements below carefully with your child and tick next to them if they agree keep these rules:

Think, then Click Early Years/Key Stage 1

These rules help us to stay safe on the Internet

I only use the internet when an adult is with us

I can click on the buttons or links when we know what they do.

I can search the Internet with an adult.

I always ask if we get lost on the Internet.

I can send and open emails together.

I can write polite and friendly emails to people that I know.

Appendix 7

Please read all the statements below carefully with your parents and tick next to them if you agree keep these rules:

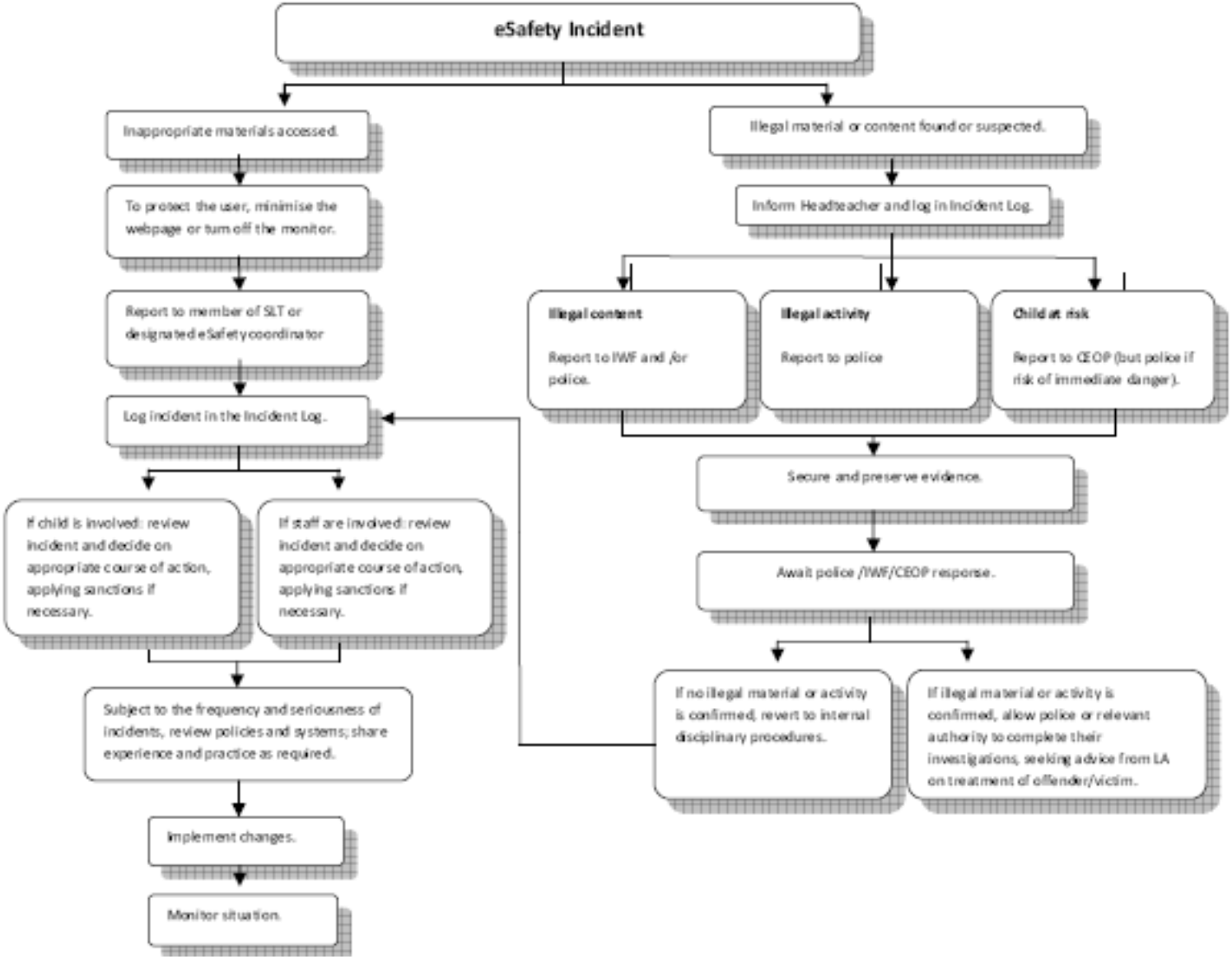
Think, then Click Key Stage 2	
e-Safety Rules for Key Stage 2	**Tick if agree**
• I will ask permission before using the Internet. • I only use websites that an adult has chosen. • I will tell an adult if we see anything I am uncomfortable with. • I will immediately close any webpage I am not sure about. • I will only e-mail people an adult has approved. • I will send e-mails that are polite and friendly. • I will never give out personal information or passwords. and I am very careful with the information that I share online • I will never arrange to meet anyone we don't know. • I do not open e-mails sent by anyone we don't know. • I do not use Internet chat rooms. • I will only open/ delete my own files • I will only use apps, programs and content which has been installed by the school.	

APPENDIX 8 – eSafety Incident Log

All eSafety incidents must be recorded by the School eSafety 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 and time of incident	Type of incident	Name/s of pupils/ staff involved	Computer details	Incident details	Resulting action taken and by whom (signed)

APPENDIX 9 – Responding to eSafety Incident/ Escalation Procedures



Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp

LCC Schools' eSafety Lead

Lancashire Schools' ICT Centre
(01257) 516360
info@ict.lancsngfl.ac.uk

Securing and Preserving Evidence – Guidance Notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system).
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
- Make a note of the date / time of the incident along with relevant summary details.
- Contact your School's Neighbourhood Policing Team for further advice.