E-Safety Policy 2025

St Augustine's Catholic Primary School

Approved by:	FGB	**Date:**	March 2025
Last reviewed on:	March 2024		
Next review due by:	March 2026		

School Mission Statement

At the heart of our Catholic faith, we pursue the truth and strive for excellence. The more we recognise and appreciate the beauty and goodness in ourselves and others, the more we come to recognise God.

At St Augustine's School, we share the Light of Christ with each other and feel a sense of belonging to the family of the Church.

Our school is a place of order, stability, tolerance and love, where we foster good relationships between home, school, parish, local and wider community.

Together we will make this school a place where everyone is nurtured, supported and valued while being circled by God's love.

When God's love enters our hearts, we grow in wisdom and understanding.

Role	**Name**	**Contact details**
Designated safeguarding lead (DSL)	Martin Kincaid	admin@staugustinesrc.lbhf.sch.uk 0207-385-4333
Deputy DSLs	Aoife Peebles Lorna Fenwick	admin@staugustinesrc.lbhf.sch.uk 0207-385-4333
Chair of Governors	John Creak	admin@staugustinesrc.lbhf.sch.uk
Local authority designated officer (LADO)	Kembra Healy	E-mail: kembra.healy@lbhf.gov.uk Telephone: 0208 753 5125 Mobile: 07776673020 Referrals: LADO@lbhf.gov.uk
Prevent Education Officer	LBHF Prevent Team	*prevent@lbhf.gov.uk* 020 8753 5727
Channel helpline	LBHF Prevent Team	*prevent@lbhf.gov.uk* 020 8753 5727

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 5
5. Educating parents about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 10
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 11
10. How the school will respond to issues of misuse 11
11. Passwords 11
12. Email use 12
13. Training 113
14. Monitoring arrangements 13
13. Links with other policies 113
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 14
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 15
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 16
Appendix 4: online safety training needs Staff audit 17
Appendix 5: online safety incident report log 18

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has

given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is: John Creak

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The IT coordinator

The IT coordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis (Turn It On)
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Staying safe online – nationalonlinesafety.com
- https://www.nspcc.org.uk/keeping-children-safe/online-safety
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

Academies that don't follow the National Curriculum should adapt this section to include details of how online safety forms part of their own curriculum.

From September 2020 **all** schools teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant such as RSHE.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this –such as E-safety day, members of the police force.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety information will also be shared during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy, anti-bullying policy and safeguarding policy)

6.2 Preventing and addressing cyber-bullying

Bullying of any kind is not accepted in our school, cyber bullying is something we take very seriously and one we will investigate and if necessary involving the police.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Sexting & sending Nude selfies

Definition of 'sexting'

There are a number of definitions of sexting but for the purpose of this advice, sexting is simply defined, as images or videos generated:

- by children under the age of 18, or
- of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know. There are many different types of sexting and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. It is important to apply a consistent approach when dealing with an incident to help protect yourself, the school and the child. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response.

Dealing with Incidents of Sexting

Steps to take in the case of an incident

STEP 1: Disclosure by a child Sexting disclosures should follow school's normal safeguarding practices. A child is likely to be very distressed, especially if the image has been circulated widely and if they don't know

who has shared it, seen it or where it has ended up. They will need support during the disclosure and after the event.

They may even need immediate protection or a referral to Referral and Assessment.

The following questions will help decide upon the best course of action:

- Is the child disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Is the school's Safeguarding Policy and practices being followed?
- For example, is the Designated Safeguarding Lead (DSL) on hand and is their advice and support available?
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the child need immediate support and/or protection?
- Are there other children and/or young people involved?
- Do they know where the image has ended up?

The situation will need to handled very sensitively to ensure the school Safeguarding and On-line Safety policies and practices are adhered to.

STEP 2: Searching a device – what are the rules?

In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device.

It is important to establish the location of the image but be aware that this may be distressing for the young person involved, so be conscious of the support they may need.

The revised Education Act 2011 brought to bear significant new powers and freedoms for teachers and schools. Essentially, the Act gives schools and/or teachers the power to seize and search an electronic device if they think there is good reason for doing so.

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography.

- When searching a mobile device, the following conditions should apply:
- The action is in accordance with the school's Safeguarding and On-line Safety policies
- The search is conducted by the Headteacher or a person authorised by them
- The DSL or a deputy is present
- The search is conducted by a member of the same sex
- If any illegal images of a child are found, you should consider whether to inform the police.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police. If an “experimental” incident is not referred to the police, the reasons for this should be recorded in writing.

Always put the child first.

- Do not search the device if this will cause additional stress to the child/person whose image has been distributed.

Never:

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the child UNLESS there is clear evidence to suggest that there is an immediate problem
- Print out any material for evidence
- Move any material from one storage device to another

Always:

- Inform the school’s Designated Safeguarding Lead
- Record the incident
- Act in accordance with school Safeguarding Policy and procedures
- Inform relevant colleagues/senior management team about the alleged incident before searching a device If there is an indecent image of a child on a website or a social networking site, then you should report the image to the site hosting it.

Under normal circumstances you would follow the reporting procedures on the respective website; however, in the case of a sexting incident involving a child or young person where you feel that they may be at risk of abuse, then you should report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

STEP 3 - What to do and not do with the image. If the image has been shared across a personal mobile device:

Always:

- Confiscate and secure the device(s)

Never:

- View the image unless there is a clear reason to do so (see above)
- Send, share, copy or save the image anywhere
- Allow children to do any of the above If the image has been shared across a school network, a website or a social network:

Always:

- Block the network to all users and isolate the image

Never:

- Send, share, copy or save the image
- Move the material from one place to another
- View the image outside of the protocols in the school's Safeguarding Policy and procedures.

STEP 4 - Who should deal with the incident?

Often, the first port of call for a child is a class teacher. Whoever the initial disclosure is made to must act in accordance with the school's Safeguarding Policy, ensuring that the Designated Safeguarding Lead (DSL) or a deputy DSL are involved in dealing with the incident.

The DSL should always record the incident using the school's Safeguarding Concerns Form. There may be instances where the image needs to be viewed and this should be done in accordance with protocols. The best interests of the child should always come first; if viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

STEP 5 - Deciding on a response

There may be a multitude of reasons why a child has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded.

It may also be necessary to assist the young person in removing the image from a website or elsewhere. Always:

- Act in accordance with the school's Safeguarding Policy
- Store the device securely
- Contact the Safeguarding in Education Team
- Carry out an Early Help Assessment in relation to the child
- Contact the police (if appropriate)
- Contact the Referral and Assessment Team
- Put the necessary safeguards in place for the child, e.g. they may need counselling support, immediate protection and parents must also be informed.
- Inform parents and/or carers about the incident and how it is being managed. Depending on the nature of the incident and the response, you may also consider contacting your local police or referring the incident to CEOP

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may not bring mobile devices into school, however, if in exceptional circumstances children may bring the device to the school. It must be given into the school office on arrival and they can collect it on the way home.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Passwords

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities.

A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Google Classroom.

Statements

- All users will have clearly defined access rights to school technical systems and devices
- All school networks and systems will be protected by secure passwords
- The administrator passwords for the school systems, used by the technical staff must also be available to the Headteacher
- Passwords for new users will be allocated by the ICT technician
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will change their passwords at regular intervals

Staff passwords

- All staff users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames
- The password should be changed at regular intervals
- The password must not include proper names or any other personal information about the user that might be known by others
- Passwords shall not be displayed on screen
- Passwords should be different for different accounts, to ensure that other systems are not put at risk
- Passwords should be different for systems used inside and outside of school

- Teachers will be provided with a password to use the school website for uploading information on the school website Pupil login
- Pupils will be taught the importance of password security

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss.

This should apply to even the youngest of users, even if class log-ons are being used

Members of staff will be made aware of the school's password policy:

The ICT technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

12. Email Use

Checking Emails

During the school day, staff should only check (or send) email when they are not teaching. Outside of the school day staff are, obviously, free to check and read their email at any time, to suit their preferred working pattern.

Sending/Replying to Emails

Emails be sent whenever suits the working hours of the staff member, however, a reply should not be expected between the hours of 6:00pm and 7:00am. This curfew is applied to encourage a better work-life balance and to make staff think more carefully about the emails they are sending. During the curfew, staff can still send emails but must not expect the recipient to reply. Further, staff should consider not replying to emails at weekends. The weekend curfew is in effect between 7.00pm Friday and 7.00am Monday.

In terms of replies to both staff and parents, we expect that any emails are responded to within a 48 hour time period. If a response is required urgently, it may be best to consider another form of contact rather than an email. A reply is not expected from staff during school holidays.

The school policy is to avoid using personal devices at home for emails. It may be unavoidable in some circumstances, when you may have to login on your personal computer. But we advise all staff to refrain from having work emails on their mobile phones/tablets or signed in on their personal computers. This is to ease the pressure on staff to constantly be replying to emails.

'All Staff' Emails

Only the headteacher and the school business manager should be emailing using the "All Staff" email list. Only send email to the relevant people. Use the 'CC' tool correctly, which is to keep other people 'looped in' with no expectation of a reply from them.

Email Etiquette Forwarding emails:

Do not forward emails without the permission of the original sender, unless they are addressed to the wrong person or should have been sent to somebody else – e.g. a question that somebody else is far more qualified to answer.

Staff and parents should have the expectation that their emails are private and will only be read by their intended recipient. Further, the recipient of the email should be aware of who else is receiving the email, so you should not "BCC" somebody else. If you wish for someone else to receive the email, please "CC" them in full sight of the recipient.

Emails sent to the School Office must, of course, be forwarded to specific people, as this is the first point of contact for many parents and outside agencies/individuals.

Language in emails:

This is a professional environment, and as such, we expect all emails to be written in a professional manner and using correct language. With email often being our first point of contact with outside agencies, it is vital we present ourselves as well as we can. As staff at a school, we are expected to have a good knowledge of the

English language and spelling. Therefore, we expect some effort to be made to email using correct grammar, punctuation and spelling, especially when interacting with parents or outside individuals.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. This will be recorded digitally once we have begun to use CPOMs.

This policy will be reviewed every year by the IT Coordinator and the headteacher. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Data Management & IT security Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

St Augustine's Catholic Primary School Acceptable Use Agreement – EYFS & KS1

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

St Augustine's Catholic Primary School Acceptable Use Agreement – KS2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors

St Augustine's Catholic Primary School Acceptable Use Agreement – Staff, Governors, Volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**