St Mark and All Saints Church of England Primary School

E-Safety Policy

TRANSFORMING SCHOOLS – TRANSFORMING LIVES
In the name of Jesus, The Good Shepherd.

Coordinator	Responsible Body
Headteacher	**Good Shepherd Trust**

Date adopted:	February 21	Last reviewed:	n/a
Review cycle:	Every 3 years or earlier	Is this policy statutory?	Yes
Approval:	Headteacher	Author:	Caroline Mallett

Revision record

Minor revisions should be recorded here when the policy is amended in light of changes to legislation or to correct errors. Significant changes or at the point of review should be recorded below and approved at the level indicated above.

Revision No.	Date	Revised by	Approved date	Comments
1	16/10/22	C. Mallett & J. Mills	16. 10.22	Updated

Introduction

The Trust, Local Committee and St Mark and All Saints C of E Primary School (We) believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that if used correctly, Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

E-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views.

Equal Opportunities

We believe it is the right of all children, regardless of their gender, religion, ethnicity, physical disability, ability, linguistic, cultural or home background, to be listened to and treated fairly whenever incidents of bullying occur.

We recognise that certain groups and individuals may be discriminated against and therefore are strongly committed to positive action to remove and counter discrimination in all aspects of the School and its work.

Aims

St. Mark and All Saints C of E Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Local Committee members
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet both in school and at home.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Work with the Trust and other schools to share good practice in order to improve this policy.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Objectives

- To ensure all members of the St Mark and All Saints community (children, staff, parents, and Local Committee members) can recognise bullying in all forms
- To ensure that there are clear strategies for the reporting of bullying, known to everyone
- To ensure that all members of our community know the strategies for dealing with bullying behaviour and implement them consistently

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for headteachers and school staff
- Relationships and sex education

● Searching, screening and confiscation

It also refers to the DfE'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 cyberbullying by, if necessary, taking possession of pupils' electronic devices and contacting the relevant services, such as the police . The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

ROLES AND RESPONSIBILITIES

Role of the Headteacher

The headteacher will ensure all school personnel, pupils and parents/carers are aware of and comply with this policy and will work closely with the coordinator and DSL to create a safe ICT learning environment by having in place:

- An effective range of technological tools
- Clear roles and responsibilities
- Safe procedures
- A comprehensive policy for pupils, staff and parents

The headteacher will:

- Ensure regular checks are made to ensure that the web filtering methods selected are appropriate, effective and reasonable
- Monitor the effectiveness of this policy
- Annually report to the governing body on the implementation of this policy

Role of the DSL

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

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

- Leading the development of this policy throughout the school
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working closely with the headteacher and the nominated Local Committee member to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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 cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Ensuring that all Internet users are kept up to date with new guidance and procedures;

- Providing guidance, support and training for all staff on induction and when the need arises 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
- Having editorial responsibility of the school website and ensuring that content is accurate and appropriate
- Ensuring regular checks are made to ensure that the web filtering methods selected are appropriate, effective and reasonable
- Undertaking risk assessments in order to reduce Internet misuse
- Keeping up to date with new developments and resources
- Undertaking an annual e-safety audit in order to establish compliance with Trust guidance
- Monitoring and reviewing this policy

Role of the IT Support Service

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

Role of All Staff and Volunteers

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

- Understanding and complying with all aspects of this policy
- Implementing this policy consistently
- Accepting the terms of the 'Responsible Internet Use' statement before using any Internet resource in school and ensuring that pupils follow the school's terms on acceptable use (appendices 1-3)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Undertaking appropriate training
- Promoting e-Safety procedures such as showing pupils how to deal with inappropriate material
- Reporting any unsuitable website or material to the e-Safety Coordinator

● Ensuring that the use of Internet derived materials complies with copyright law

Role of Pupils

Pupils will be aware of this policy and will be taught to:

● Be critically aware of the materials they read

● Validate information before accepting its accuracy

● Acknowledge the source of information used

● Use the Internet for research

● Respect copyright when using Internet material in their own work

● Report any offensive e-mail

● Report any unsuitable website or material to the e-Safety Coordinator

● Access the internet safely

Role of Families

● Access the internet safely

● Be made aware of this policy

● Be asked to support the e-Safety policy and to sign the consent form allowing their child to have Internet access

● Make sure their children has read, understood and agreed to the terms on the e- safety policy acceptable use of the school's ICT systems and internet

● Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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

● What are the issues? – UK Safer Internet Centre

● Hot topics – Childnet International

● Parent resource sheet – Childnet International

● Discuss aspects of this policy during the year

Role of School Council

● Discuss aspects of this policy during the year

Role of 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).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum using The National Curriculum computing programmes of study and the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Cyberbullying

Cyberbullying 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.) cyberbullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology.

• It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people.
• It can take place across age groups and target pupils, staff and others.
• It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.
• It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyberbullying may be carried out in many ways, including:
• Threatening, intimidating or upsetting text messages;

• Threatening or embarrassing pictures and video clips via mobile phone cameras;
• Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
• Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
• Menacing or upsetting responses to someone in a chat-room;
• Unpleasant messages sent during instant messaging;
• Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook)
In some cases this type of bullying can be a criminal offence.

Prevention of Cyberbullying

To help prevent cyberbullying, 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.

- Pupils will be informed about cyberbullying through curricular and pastoral activities. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- The Head will act, as the e-Safety Officer, to oversee the practices and procedures outlined in this policy and monitor their effectiveness.
- The e-Safety Officer will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.
- All staff, Local Committee members and volunteers (where appropriate) receive training on cyberbullying, to identify signs of cyberbullying, its impact and ways to support pupils and will be helped to keep informed about the technologies that children commonly use as part of safeguarding training.
- A Code of Advice (see Appendix 1) will be developed, periodically reviewed and communicated to help pupils protect themselves from being caught up in cyber bullying and to advise them on reporting any incidents.
- Pupils and staff are expected to comply with the school's Acceptable Computer Use Policy
- Parents will be provided with information and advice on cyberbullying
- In relation to a specific incident of cyberbullying, 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or

- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The School behaviour policy

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

Internet Use

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 to 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 to 3.

Internet use is designed for pupils in the following ways:
▪ Includes school web filtering technology configured, provided and approved by the Trust which is designed to protect pupils from unsafe materials on the internet;
▪ Provides web filtering which is reviewed annually and improved if necessary;
▪ Includes web filtering appropriate to the age of pupils;
▪ Has virus protection software installed which will be updated regularly;

Authorising Internet Access

Before using any school ICT resource, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement'
▪ Parents must sign a consent form before their child has access to the Internet.
▪ An up to date record will be kept of all pupils and school personnel who have Internet access.

Email

Pupils must:
▪ only use approved e-mail accounts;
▪ report receiving any offensive e-mails;
▪ not divulge their or others personal details;
▪ not arrange to meet anyone via the e-mail;
▪ seek authorisation to send a formal e-mail to an external organisation
▪ not take part in sending chain letters

Social Networking

Pupils will not be allowed access:
▪ to social networking sites except those that are part of an educational network or approved Learning Platform;
▪ to newsgroups unless an identified need has been approved

Pupils using mobile devices in school

Pupils may not bring mobile devices into school, and are not permitted to mobile devices use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Mobile phones will be confiscated and will be held securely until an adult family member makes arrangements to collect them.

Under exceptional circumstances and with agreement with the headteacher, a pupil may bring a mobile device to school, for example if they need it in order to be safe when travelling a long distance home. In this case, the device will be held in the school office until home time.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the headteacher and the IT Support Service.

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 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.

Inappropriate material

Any inappropriate websites or material found by pupils or school personnel will be reported to the e-Safety Coordinator who in turn will report to the Internet Service Provider.

School Website

Contact details on the website will be:
▪ the school address
▪ e-mail address
▪ telephone number
The school website will not publish:
▪ staff or pupils contact details;
▪ the pictures of children without the written consent of the parent/carer;
▪ the names of any pupils who are shown;
▪ children's work without the permission of the pupil or the parent/carer

Internet System Security

▪ New programs will be installed onto the network or stand alone machines by the IT Support Service technicians
only.
▪ Personal storage, CD's and other data record devices may not be used in school.
▪ Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

Local Committee members 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.

Monitoring arrangement

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the e-Safety coordinator. At every review, the policy will be shared with the Local Committee. The review will be supported by an annual risk assessment that considers and

reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

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
- ICT and internet acceptable use policy

Complaints

The headteacher will deal with all complaints of Internet misuse by school personnel or pupils. Parents/carers will be informed if their child has misused the Internet.

Cyber Safety Code

Three Steps to Safety

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including phone numbers or passwords.
2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.
3. "Do as you would be done by!" Think how you would feel if you were bullied. You are responsible for your behaviour - so don't distress other people or encourage others to do so.

If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Don't reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists, you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to your mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don't accept emails or open files from people you don't know.
- Don't delete bullying emails – print them or save them as evidence in a separate folder.

<u>Social networking sites, chatrooms and instant messaging</u>

• Change privacy settings so you can choose who to be friends with and who can see your profile. Don't add anyone you don't know to your friend list.

• Don't use your real name in chatrooms.

• Never give out your photo or personal details, like your address, phone number or which school you go to.

Don't post any pictures or videos you wouldn't be happy for your parents or teachers to see. Once they are online, they can be copied and posted in other places where you can't get rid of them.

• Keep your passwords private and don't tell anyone, not even your best friend.

• To report suspicious behaviour online and to learn more about keeping yourself safe online visit www.thinkyouknow.co.uk

Always report bullying incidents. Not doing that allows the bully to continue. That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behaviour

Acceptable Use

Agreement / eSafety Rules

- ✔ I will only use ICT in school for school purposes.
- ✔ I will only use my class email address or my own school email address when emailing.
- ✔ I will only open email attachments from people I know, or who my teacher has approved.
- ✔ I will not tell other people my ICT passwords.
- ✔ I will only open/delete my own files.
- ✔ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✔ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✔ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
- ✔ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✔ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✔ I know that my use of ICT can be checked and that my parents/carers can be contacted if a member of school staff is concerned about my eSafety.

Appendix 2

E-Safety Audit – Primary Schools

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update: October 22	
The Policy was agreed by the Headteacher in February 2021	
The Policy is available for staff at: Subject Leadership/ Information/Computing	
And for parents on the policies page of the school website	
The designated Safeguarding Lead is: Mrs Caroline Mallett	
The e-Safety Coordinator is: Miss Jess Miller	
Has e-safety training been provided for both pupils and staff?	Y
Is the Think U Know training being considered?	Y
Do all staff sign an ICT Code of Conduct on appointment?	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y
Have school e-Safety Rules been set for pupils?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y
Has the school filtering policy been approved by GST?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Accepted for school: St Mark and All Saints C of E Primary School

Referral Process

Appendix 4