E-safety Policy

Costock CE Primary School

Every Child's a Star!
'As God's children, we shine like Stars' Philippians 2 v.15

Our Promise

Every day at Costock Church School we are experiencing and learning;

Service to God, each other and ourselves, Truth, Agape and Respect

As we leave each day we take these Christian Values with us

Approved by:	C&P	**Date:**	4th March 2023
Last reviewed on:	Spring Term 2022		
Next review due by:	Spring Term 2024		

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.

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, sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The e-safety policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and Safeguarding children. The policy and its implementation will be reviewed annually.

Roles and responsibilities

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

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

The designated safeguarding lead:
Details of the school's DSL [and deputy/deputies] are set out in our child protection and safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (Appendix 6) 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 and anti-bullying policy.
- Ensuring staff training for on online safety is up to date
- Liaising with other agencies and/or external services if necessary

E-Safety Co-ordinator:
The school has an e-safety coordinator. Our coordinator is: Hollie Benson.

ICT Service Provider:
The ICT service provider 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
- Monitoring the school's ICT systems on a daily basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged (Appendix 6) 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

Parents
Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- All pupils and parents are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet based on the Key Stage the pupil is currently in. See "Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers" (Appendices 1-2).

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet - Childnet International

Visitors or 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 by signing the appropriate agreement (Appendix 3)

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.

- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Remote learning protocols
In order to facilitate remote learning, all pupils will be supplied with an individual costock.notts.sch.uk e-mail address and Microsoft Teams is the chosen platform for delivering live online sessions. All pupils will be made aware of the Pupil Code of Conduct for Remote Learning (appendix 4) and will be asked to sign to acknowledge that they have read or been told about the code and agree to adhere to it. This includes the 'Microsoft Teams Session Preparation and Conduct' (appendix 5).

Managing Internet Access

Information security system
- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail
- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform (eg Purple Mash) and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website
- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published
- The headteacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified. Group photographs will be used rather than full-face photos of individual children.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the school website
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations 2016

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form which is an integral part of the "Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers" (Appendices 1 & 2).
- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site

Acceptable use of the internet in school

- All staff are expected to read and sign the Acceptable Personal Use of Resources and Assets Policy (Appendix 6)
- All pupils and parents are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet based on the Key Stage the pupil is currently in. See "Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers" (Appendices 1 & 2).
- 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 and visitors (where relevant) to ensure they comply with the above.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the headteacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Pupils using mobile devices in school

- Pupils may bring mobile devices into school in exceptional circumstances agreed with school and must hand them into the school office on arrival at school and collect them from the school office at the end of the day.
- Pupils are not permitted to use mobile devices during lessons or during after school club or any other activities organised by the school
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Communicating the policy

Pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all classrooms (see Appendices 8 & 9)
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be shown where to access the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines on induction and annually thereafter.

- Staff should be aware that the system is monitored and that professional standards are expected.

Parents

- The Policy will be published on the school website
- All parents will be asked to sign the parent/pupil agreement when they register their children and when they move from Early Years/KS1 to KS2.

Links with other policies

This e-safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF PUPILS IN EYFS AND KS1	
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)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF PUPILS IN KS2	
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 **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 3

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR GOVERNORS, VOLUNTEERS AND VISITORS	
Name of 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) 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

Costock C of E Primary

Pupil Code of Conduct for Remote Learning

- I will only use my school email account for school work.
- I will only take part in 'live' sessions through my school Teams account as part of a lesson set up by a member of school staff.
- I will be responsible for my behaviour and actions when using technology (e.g Microsoft Teams, Purple Mash and other interactive applications). This includes the resources I access and the language I use.
- I have read and understand the school's 'Microsoft Teams Session Preparation and Conduct' document.
- I will make sure that all my communication with other children, teachers or others using technology is responsible and sensible.
- I will not deliberately browse, download, upload or forward material that could be considered offensive. If I accidentally come across any such material I will report it immediately to my teacher or my parent.
- I will not share resources or videos created by my teachers with anyone who is not a pupil or member of staff
- I will not share any school content on social media platforms.
- I understand that when sending and receiving emails through my school email account my use will be monitored.
- I will continue to follow the rules regarding my use of technology as outlined in the school's 'Acceptable Use of the School's ICT systems and Internet Agreement 'that I have signed.
- I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted.

To be returned to school

Pupil: I _____ (insert pupil name here) have read, understood and agree to the terms set out in the above Code of Conduct.

Signed (Pupil):
Date:

Signature of Parent or Teacher who discussed this with the pupil: _____

MICROSOFT TEAMS SESSION PREPARATION AND BEHAVIOUR

By taking part in Microsoft Teams sessions, you are agreeing to the following statements:

- I will remember that all the normal school rules apply when I am learning online. If these are not followed, I will be removed from the session and my parents informed.
- I will not record or take photos of my classmates or teachers in the session.
- I will only join in conversations when my teacher tells me to; I will keep my microphone muted and my camera switched off until my teacher tells me to switch them on.
- I understand that when on a Teams session that my activity can be monitored and logged by my teachers.
- I am aware that when in a live Teams session this is an extension of the classroom and I should behave as I would in a classroom.

BEFORE THE SESSION

Have your session in a quiet, safe and shared place (preferably not a bedroom).

Be on time and mute your microphone when joining.

Be dressed appropriately for learning (no pyjamas).

DURING THE SESSION

Follow the instructions of your teachers during these live sessions.

Interact patiently and respectfully with your teachers and classmates.

Don't use the chat function unless asked to do so by your teacher.

Remain attentive during the sessions without distraction.

Live sessions may be recorded by the teacher for safeguarding reasons; any inappropriate behaviour will therefore also be recorded.

Any pupil who behaves inappropriately by not following any of these rules will be removed from the session and may be excluded from future live sessions and parents contacted.

Appendix 6

Acceptable Personal Use of Resources and Assets Policy

Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use

What must I do?

1. ***MUST***: You must use our facilities **economically**; your personal use must not create extra costs for us
2. ***MUST NOT***: You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
3. ***MUST NOT***: Personal use must not interfere with your **productivity** and how you carry out your duties
4. ***MUST NOT***: Personal use must not reflect adversely on our **reputation**
5. ***MUST NOT***: You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them
6. ***MUST NOT***: You must not use browsers or access/ attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
7. ***MUST NOT***: You must not **send or forward** chain, joke or spam emails
8. ***MUST NOT***: You must not use the Organisation's facilities for **commercial purposes** not approved by us or for personal financial gain
9. ***MUST NOT***: You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
10. ***MUST NOT***: You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
11. ***MUST NOT***: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information **unattended**.
12. ***MUST NOT***: You must not **connect** any equipment to our IT network that has not been approved
13. ***MUST NOT***: You must not do anything that would **compromise** the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings
14. ***MUST NOT***: You must not make personal use of the information available to you that is not available to the **public**

Why must I do it?

1. ALL: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes

How must I do it?

1. By checking with your manager or where you have any uncertainty over what is appropriate
2. By complying with the points of this policy
3. You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours'
4. By complying with the points of this policy
5. Closing websites when you are not actively using them
6. By taking care over the sites you are about to open, including reading search report information before opening
7. By deleting such items if you receive them.
8. By checking with your manager where you have any uncertainty over what is appropriate
9. By checking with your manager where you have any uncertainty over what is appropriate
10. If you are not sure if you are authorised to disclose information, speak with your manager in the first instance
11. If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
12. Check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection.
13. IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
14. If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 7

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**

Appendix 8

E-safety rules for EYFS and Key Stage 1

Think then Click

These rules help us stay safe on the Internet

- I only use the internet when an adult is with me
- I can click on the buttons or links when I know what they do

- I can search within websites chosen by an adult
- I always ask if I get lost on the internet

- I can send and open e-mails with adult help
- I can write polite and friendly e-mails to people that I know

Appendix 9

E-safety rules for Key Stage 2

Think then Click 

- I will only use the internet if I have permission
- I will only use websites that an adult has chosen
- I will tell an adult if I see anything I am uncomfortable with
- I will send and post messages and comments that are polite and friendly
- I will never give out passwords or personal information
- I will not open e-mails sent by anyone I don't know
- I will not use internet chat rooms
- I will never arrange to meet anyone new that I have only chatted with on-line