E-Safety Policy

Mission Statement (5 Promises)	
Keep Everyone *LEARNING*	*Because God calls us to fullness of life in Christ we provide varied exciting opportunities for children to achieve highly.* God invites us to promise; **to keep everyone learning**
Keep Everyone INCLUDED	*Because God calls us to love our neighbour we respect and include each other and develop the skills of confidence, resilience, independence, empathy and understanding.* God invites us to promise; **to keep everyone included**
Keep Everyone SAFE	*Because God shows us the best way to live we get to know ourselves and learn how to be safe.* God invites us to promise; **to keep everyone safe**
Look After the World Around Us	*Because God calls us to live as faithful members of the community we respect the world around us.* God invites us to promise; **to look after the world around us**
Be Honest	*Because God calls us to be like him we get to know ourselves and learn to respect the truth.* God invites us to promise; **to be honest**

Approved by:	Approval Date:	Review Date:
SDC	19th July 2021	Summer 2022

IT has an all-encompassing role within the lives of children and adults. Internet and online technologies are enhancing communication and the sharing of information. These mostly positive technologies have brought around emerging threats to the welfare of pupils' physical and emotional health.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- e-mail
- Instant messaging sometimes using simple web cams e.g. Facebook Messenger WhatsApp, snap chat, tiktok, Instagram
- Web based voice and video calling e.g. Skype / Zoom / Teams
- Online chat rooms and forums Roblox / Adopt Me
- Social networking sites e.g. Facebook
- Blogs and Micro-blogs e.g. Twitter / Instagram
- Podcasting
- Video broadcasting sites e.g. You Tube / Instagram
- Music and video downloading e.g. iTunes
- Smart phones with e-mail, messaging, photos and internet access

Our whole school approach to the safe use of IT

A safe IT learning environment includes four main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum and schemes of work
- Safe and secure broadband for Learning including the effective management of content filtering.

E-Safety Audit – Primary Schools

This quick self-audit will help the leaders in school 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: 19/07/2021	
The Policy was agreed by governors on: 19/07/2021	
The Policy is available for staff at: Policies and Proceedures (O:)	
And for parents at: School office and website	
The designated Child Protection Teachers/Officers are: Mr Chris Bratt Mr Richard Hinchliffe	
The e-Safety Coordinator is: **Mr C Bratt**	
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 a 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 DCSF requirements for safe and secure access.	**Y**
Has the school filtering policy been approved by SLT?	**Y**
Is personal data collected, stored and used according to the principles of GDPR?	**Y**

School E-Safety Policy

The e-safety coordinator is the DSL and ensures that safety procedures are monitored and reviewed. Our e-Safety Policy has been written by the school following Government and Local Authority guidance. It has been agreed by the school staff and approved by governors.

The e-Safety Policy will be _reviewed annually_. This policy will next be reviewed in Summer 2022.

This policy should be read in conjunction with the Anti-bullying and Behaviour and Physical Intervention policy. Staff should also read in conjunction with the staff code of conduct.

This policy refers to CPOMs. This is an electronic monitoring and reporting system which allows school to record information about a child in a secure way. Categories are determined by the school and include child protection, safeguarding, welfare and pastoral concerns.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:
- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF;
- access to learning at all times

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school authorises all staff working in school internet access.
- All staff must read and sign to say they have read the school code of conduct and staff handbook which refers to acceptable IT use before using any school IT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent statement in the pupil information form which refers to the home school agreement; detailing pupil access in the E-safety policy. (School Planners / Sims Data Collection)

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the IT network manager Sam Taylor samtaylor@jasmineit.org.uk who will contact the Local Authority.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail / message.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved. This school uses Facebook for communication and Teams for virtual meetings / lessons.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible. If a site is filtered the following screen will appear.

Video Conferencing

- Teams has been used to support remote learning and is the preferred platform at this school.
- Links are given directly to parents and children can log on using these links provided.
- Lesson times and content vary according to age of child.

Managing Emerging Technologies

- Staff may use their own device if appropriate measures are taken through the 'Bring your own device' Policy.
- Mobile phones will not be used for personal use during lessons or formal school time.
- The sending of abusive or inappropriate text / WhatsApp messages is forbidden.
- Older pupils may bring phones but these must be handed in to staff and given back at the end of the day.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Web or Facebook page, particularly in association with photographs.
- This policy should be read in conjunction with the school GDPR Policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and Jasmine IT.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR Policy.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Nottinghamshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Liaison officers to establish procedures for handling potentially illegal issues.
- Incidents of misuse will be recorded on the school electronic recording system CPOMS

Curriculum

- Internet Safety is taught in school.
- Resources are saved on the T Drive – 9. Curriculum / IT / Internet Safety
- Additional lessons are taught as concerns arise.

Communication of Policy

Pupils
- Rules for Internet access will be posted in all rooms.
- Pupils will be informed that Internet use will be monitored.

Staff
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents
- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Websites to support parents and teachers in keeping children safe on line are below.

https://www.thinkuknow.co.uk/

https://www.ceop.police.uk/Safety-Centre/
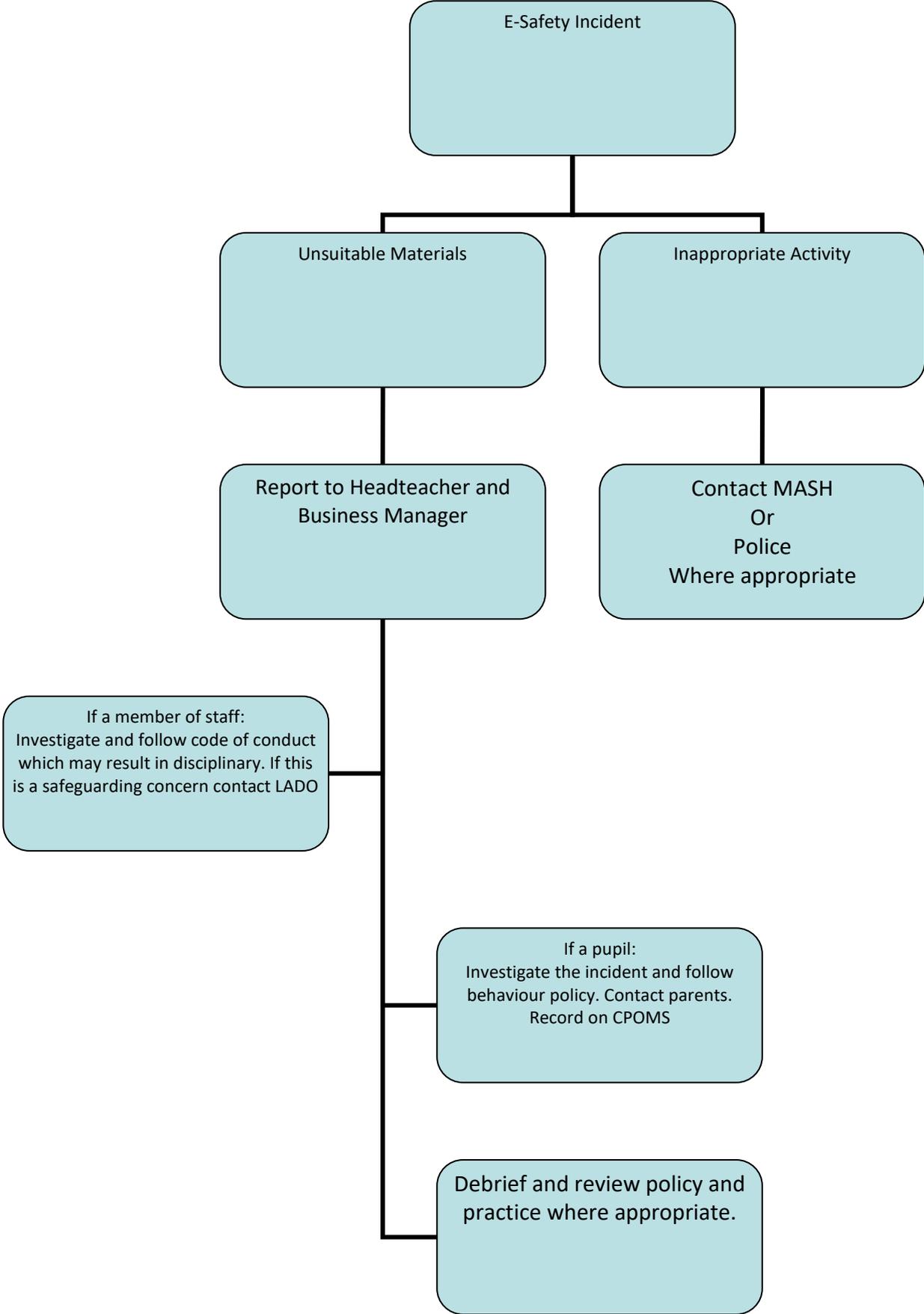
Referral Process – Appendix A

E-Safety pupil acceptable use agreement Rules– Appendix B

E-Safety parent/carer acceptable use agreement – Appendix C

Staff information Code of Conduct – Appendix D

Flowchart for responding to e-safety incidents in school

E-Safety Incident

Unsuitable Materials

Inappropriate Activity

Report to Headteacher and Business Manager

Contact MASH
Or
Police
Where appropriate

If a member of staff:
Investigate and follow code of conduct which may result in disciplinary. If this is a safeguarding concern contact LADO

If a pupil:
Investigate the incident and follow behaviour policy. Contact parents. Record on CPOMS

Debrief and review policy and practice where appropriate.

Appendix B

Key Stage 1 E-Safety pupils acceptable use agreement

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

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

We can search the Internet if an adult is present.

We always ask if we get lost on the Internet.

Key Stage 2

Think then Click
E-Safety Acceptable Use Agreement - Rules for Key Stage 2

- We ask permission before using the Internet.

- We only use websites that an adult has chosen.

- We tell an adult if we see anything we are uncomfortable with.

- We immediately minimise any webpage we not sure about.

- We will learn how to use the '**thinkyouknow'** website to keep ourselves safe.

- We send messages that are polite and friendly.

- We never give out personal information or passwords.

- We never arrange to meet anyone we don't know. We are aware of stranger danger and only message people an adult has approved.

- We do not open messages sent by anyone we don't know.

- We do not share personal information about ourselves or others without permission.

- We know the school can look at what we see online.

- We respect our computer equipment and the work of others and we don't upload or download images, music or videos without permission.

- We do not use mobile phones in school or USB devices without permission.

- We do not fill out any online forms without adult permission

- We will learn about copyright laws and make sure we acknowledge resources we use.

- We understand these rules help us both in school and outside school.

E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.

- It is a criminal offence to use a computer or network for a purpose not permitted by the school.

- Irresponsible use may result in the loss of network or Internet access.

- Network access must be made via the user's authorised account and password, which must not be given to any other person.

- All network and Internet use must be appropriate to education.

- Copyright and intellectual property rights must be respected.

- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.

- Anonymous messages and chain letters are not permitted.

- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.

- The school IT systems may not be used for private purposes, unless the head teacher has given specific permission.

- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

E-safety
Parent/Carer Acceptable Use Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to read these rules and sign the pupil information form which states that they understand and accept the contents of the home-school agreement, including E-Safety Rules.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. I will not post pictures taken of other children in school on social networking sites.

Parent's Consent for Internet Access

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

I understand that occasionally inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise according to the policy.

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

I understand that my son's/daughters activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the e-safety rules.

I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate or malicious comments about the school or any member of the school community

<u>Staff Information Code of Conduct</u>

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'.

Name (Print):

Signed:

Date: