Marton Manor Primary School
E-Safety Policy

This policy was formulated in consultation with staff and governors at Marton Manor Primary School. It was last reviewed in Autumn 2020.
Please read in conjunction with our Remote Learning policy and Child Protection policy.

The e-Safety Policy will be reviewed annually by the Governing Body.

This policy will next be reviewed in Autumn 2021

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the National Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.
  - This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.
-

E-Safety Audit – Primary Schools Has the school an e-Safety Policy that complies with CYPD guidance?	**Y/N**
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	**Y/N**
Is the Think U Know training being considered?	**Y/N**
Do all staff sign an ICT Code of Conduct on appointment?	**Y/N**

Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y/N**
Have school e-Safety Rules been set for pupils?	**Y/N**
Are these Rules displayed in all rooms with computers?	**Y/N**
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	**Y/N**
Has the school filtering policy has been approved by SLT?	**Y/N**
Is personal data collected, stored and used according to the principles of the latest Data Protection Act?	**Y/N**

Contents

School e-Safety Policy

The school has an e-Safety leader. The Designated Child Protection Officer and her deputies will also provide e-safety support as the roles overlap.

Our e-Safety Policy has been written by the school, building on Government guidance. It has been agreed by the senior leadership team and approved by governors.

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 DFE; access to learning wherever and whenever convenient.

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.
- Pupils will regularly learn about E-Safety across the computing curriculum, they will participate in externally led workshops (www.ecplimited.com) on how to make best and safest use of modern technology.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the One IT helpdesk via the e-safety leader or Head Teacher.

- 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.
- 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.

- 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, One IT and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones to school are required to hand them in to the school office staff every morning and devices are collected at home time.

The Prevent Duty and E-Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

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 head teacher 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 and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

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 One IT

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the latest Data Protection Act .

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 James Cook Learning Trust can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT 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 Head teacher.
- 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 where there is a need to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked 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.
- All staff will be trained in Safeguarding procedures, including elements of ESafety and The Prevent Duty.
- 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. The school will also organise E-Safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Referral Process – Appendix A

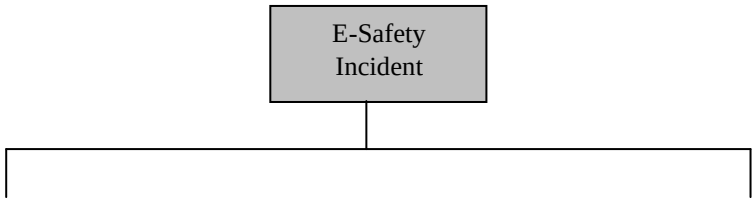
E-Safety Rules– Appendix B

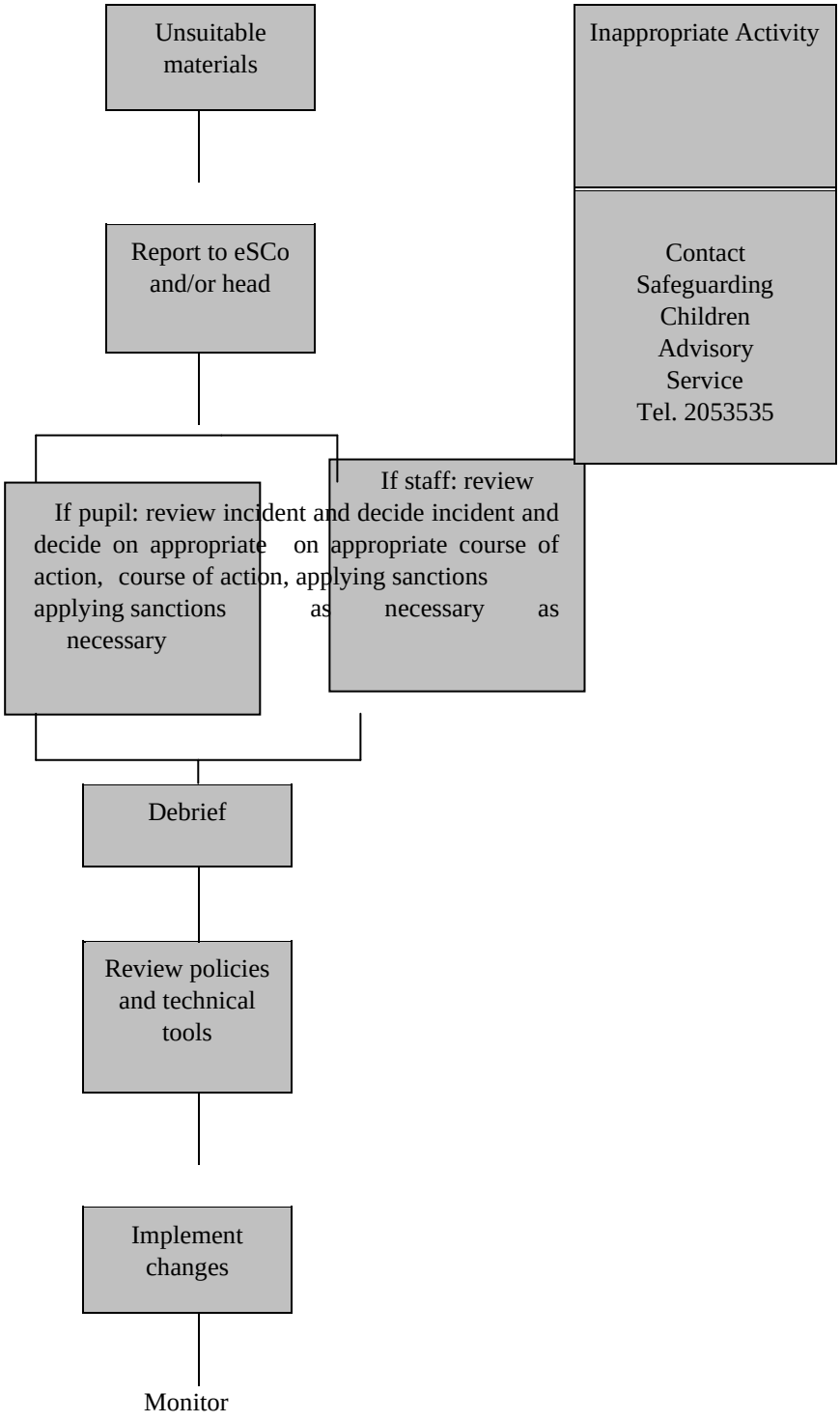
Letter to parents – Appendix C

Staff Acceptable Use Policy – Appendix D

Appendix A

Flowchart for responding to e-safety incidents in school





Adapted from Becta – E-safety 2005

Appendix B

KS1 E-SAFETY RULES

☺ 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 with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

KS2 E-SAFETY RULES

These rules help us to stay safe on the Internet

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 close any webpage we are not sure about.

We only email people an adult has approved.

We send emails that are polite and friendly.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

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

We do not use internet chat rooms.

Marton Manor 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 ICT 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.

Dear Parents and Carers

As part of our Information Communications and Technology scheme of work and general curriculum enhancement, Marton Manor school is providing supervised access to the Internet and e-mail. We are confident that this will benefit our children and equip them with important skills and knowledge in the wider world.

Our Internet Service Provider, overseen by One IT , operates a filtering system that restricts access to inappropriate material. Children will always be supervised when using the Internet, and the rules of responsible Internet use will be explained to them at school.
The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the James Cook Learning Trust can accept liability for material accessed, or any consequences of Internet access.

To support the policy, we ask you to sign the enclosed agreement. It would be helpful also if you would talk to your child about the 'rules' whenever necessary. Should you wish to discuss this agreement or any aspect of the Internet use, please contact me to arrange an appointment.

Yours sincerely

,
Head Teacher

Marton Manor Primary School

Information and Communications Technology Acceptable use of Internet Agreement

Pupil and Parent Agreement

When I use the Internet and e-mail at school, I will keep to these rules:

- I will only use the Internet with permission, when there is a teacher or adult helper present.
- I will not try to find unsuitable sites on the Internet
- I will only e-mail people I know, or who my teacher has approved
- The messages I send will be polite and sensible
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent, carer, or teacher has given permission.

Pupil's signature …….. **Date:** ……

Parent

As the parent or legal guardian of the pupil signing above, I give permission for my son or daughter to use electronic mail and the Internet, under supervision at school.

I understand and accept the above rules for acceptable use of the Internet and will discuss these with my child.

Parents' signature …… **Date**……

Pupil's name ……

Class ……

APPENDIX D: 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 rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- 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.
- will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety leader or the Designated Child Protection leaders.
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- 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: …… Capitals: ……