Internet Safety Policy

Person responsible: Headteacher
Ratified by the governing body: Spring 21
Date for review: Spring 24

Reverend Anne-Marie Renshaw
Chair of governors

1. Rationale

The Internet is so prevalent in children's lives and there are significant educational benefits that can result from its usage within the curriculum, including access to research material from around the world and the abilities to publish and communicate information to a wider audience.

Safe Internet usage depends on all stakeholders within Messing Primary School, staff, governors, advisers and parents taking responsibility for the use of the Internet.

- The Internet is an essential element in 21st Century life for education, business and social interaction. Messing Primary has a duty to provide children with quality Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.
- Benefits of using the Internet allows access to world-wide educational resources including museums and art galleries, and the teaching staff will apply a professional reasonable precaution to ensure that users will only access appropriate material for these needs.
- Safety prompts for Internet access will be posted near all computers.
- Anti-virus software to protect the school's computer assets will be installed and updated regularly.
- Parents and staff will be provided with regular updates about Internet Safety and the latest information or where to find support.

2. Scope of the Policy

This policy applies to all members of Messing Primary school, including anyone using the systems (including volunteers).

The policy should be used to enable all members of Messing Primary School to adopt an appropriate and professional e-safety environment together. The policy should also aid reporting and monitoring of any e-safety issues within the school environment.

Messing school will deal with such incidents appropriately as is written in this policy along with anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school. These issues will also be included within the teaching of online safety during computing lessons to ensure they are addressed as part of the digital literacy curriculum.

3. Roles and responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Internet Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Governing body will include e-safety in their monitoring of child protection and safeguarding within the school. This will include:

- regular meetings with the designated safeguarding lead, including e-safety issues.

- regular monitoring of e-safety incidents.
- reporting regularly on e-safety at the full Governing body meeting.

Head teacher/ Computing leader:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety.
- The Head teacher and computing leader are responsible for the day to day e-safety issues.
- The Headteacher and Deputy designated safeguarding lead is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or the Headteacher.
- The Headteacher and staff team will receive regular updates from the Computing subject leader regarding e-safety in the school and will act upon issues where required.

Computing Subject leader:

- reviews Messing School e-safety policies / documents in co-ordination with the Head teacher.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff about the latest internet safety information.
- liaises with the technician and office manager regarding any computing problems and queries.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with the Head teacher (designated safeguarding lead) to discuss current issues, review incident logs and recommend any future developmental needs.
- informs relevant Governing Body meetings to report any issues and report on the success of e-safety within the school.

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the **Staff Acceptable Use Policy**
- they report any suspected misuse or problem to the Headteacher
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- internet safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the **internet safety policy** and the **Responsible Internet and Computer Use Agreement**
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Pupils:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety and anti-bullying policies covers actions out of school, if related to their membership of the school (eg. Involving another member of school or a piece of equipment)
- are responsible for using all school systems in accordance with the **Responsible Internet and Computer Use Agreement** including guidance on preventing cyber-bullying.

This is discussed with pupils at the start of each school year and each pupil signs the class copy of the agreement. This is then displayed and referred to throughout the year.They are also sent out to parents at the start of the year.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

Messing School will take every opportunity to help parents understand these issues through newsletters, letters, the school website, training dates and literature available at reception and sent home regularly with children.

Parents and carers will be encouraged to support Messing School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Safe use of the internet and appropriate use of age restricted/ Social Media sites
- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

4. Internet safety within the curriculum:

Introducing e-safety Policy to Pupils, Staff and Parents

The importance of e-safety will be taught explicitly as part of our Computing/PSHE curriculum and will be planned in accordance to the age, maturity and understanding of the children.

All staff will be given the e-safety policy and its importance explained.

Parents' attention will be drawn to the school e-safety policy in newsletters, and on the school website, where appropriate suitable materials to support parental understanding and awareness will be available.

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid safety risks and build their resilience.
E-safety will provided within the school in the following ways:

- Regularly planned e-safety lessons should be part of the computing curriculum and included on the computing provision map.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the **Responsible Internet and Computer Use Agreement** and encouraged to adopt safe and responsible use both within and outside school

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and encourage the use of the search engine 'Safe search' where possible.
- Children in Year 6 to be taught the dangers and effects of 'sexting' upon themselves and the people around them. This is to be taught with parental communication to ensure all parties involved know how important this is but that it is taught with in line with the school *Relationships and sex education Policy.*

Internet safety for parents/carers:

The Internet can be a fast paced piece of technology that is ever evolving and with this in mind, the school will help parents to understand the positive and negative effects of Internet sites upon children if used in the correct and incorrect ways.
This will be by:

- Meetings
- Letters
- Information available at the Reception area
- Events such as 'safer internet' days
- Website promotion for parents to use as referenced in the appendix
- Open access to teachers regarding any concerns after school

Internet safety for staff:

It is highly important that staff receive appropriate training and understanding as to the importance of e-safety in all daily activities. Training will be regularly provided to ensure this and an open door policy to raise any concerns the Head Teacher or Computing Subject leader.

The e-safety policy will be discussed and reviewed with staff and any concerns are reported on a safeguarding concerns sheet.

Staff will be trained on how important the **Staff Acceptable Use Agreement** is and encouraged regularly to understand and adhere to its contents.

Staff should be aware that the School reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means. Under no circumstances should pupil-named data be transmitted over the Internet or email. The School office has use of encrypted data systems for this purpose.

Social media for staff:

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Photographs posted on sites should not cause the school or themselves embarrassment
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They are fully aware of guidelines in the staff hand book.

5. Principles for Acceptable Use of the Internet

Use of school computers by pupils will be in support of the aims and objectives of the National Curriculum.

Online activities which are encouraged include:

- The use of email and computer conferencing for communications.
- Use of the Internet to investigate and research school subjects, cross- curricular themes or topics related to social and personal development.
- The development of pupils' competence in ICT skills and their general research skills.

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum or future careers.
- Using social network sites to make comments about the school, children, parents, governors and school policies.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering and goods or services, unless specifically approved by the school.
- Playing computer games or using other interactive 'chat' sites unless specifically approved by the school.
- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a use (such as: home address; email address; phone number; etc).
- Downloading software.
- Any activity that violates a school rule.

5. Guidelines

Children will:

- have equal access to email in a safe and secure environment
- have equal access to a variety of approved websites through the Internet
- be taught all the skills in order to use Internet and email as an ICT tool
- use Internet and email to support, enhance and develop all aspects of curriculum
- develop Internet and email skills at the appropriate level for all.

Guidance for All Users

All staff at Messing Primary are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others on the education world. Electronic information- handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Internet.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.

Pupils are responsible for their good behaviour on the school networks, just as they are on and off school premises.

Staff should ensure that pupils know and understand that activities not permitted are to:

- Retrieve, send, copy or display offensive messages or pictures.
- Use obscene or racist language.
- Harass, insult or attack others.
- Damage computers, computer systems or computer networks.
- Violate copyright laws.
- Use another user's password.
- Trespass in another user's folders, work or files.
- Use the network for commercial purposes.

6. Photographs in School

At Messing Primary we have taken a sensible, balanced approach to photographs and videoing in schools and schools activities outside the school.
We recognise that parents want to capture significant moments on camera and it is usual for parents to take photographs and videos of children at school events such as concerts, class assemblies and sports day. In addition, making use of photographs in school and in the media can help increase pupil's motivation and help parents and the local community identify and celebrate the academy's achievements. However, photographs must be used in a responsible way and we need to respect pupils' and parent's rights of privacy and be aware of potential child protection issues. Our view is that potential risk can be minimised by the following good practice:

- The school always asks for parental consent before using images of pupils, via the parental consent form as part of the registration process when the child starts school.
- The school will always abide by parent/carers' requests and will also allow parents to withdraw their child from certain activities where it is impossible to

guarantee their child will not be included in another parent's photographs by accident (for example crowd shots on sports day and concerts.)

- Parents should under no circumstances download any child's image (other than their own children if they so wish) onto any social networking site. It has been known for children placed in refuges for their own safety, or in foster care for example, to be located as a result of their photograph appearing in a newspaper and so clearly this possibility also exists should images appear on the internet.
- If parents have any concerns about inappropriate or intrusive photography, they should report them to the Headteacher who will follow them up in the same manner as any other child protection concern.

7. Use of Mobile Phones:

Adults working within the school are allowed to bring mobile phones on site. However, they must be left in the school office or staff room.
The code of conduct states that:

9.1 Employees are required to ensure mobile telephones are switched off/switched to silent during working hours. Employees are not permitted to use their mobile telephones during working hours, and must ensure they are stored securely and are not accessible by pupils at any time.

9.2 Employees are not permitted to contact pupils by telephone, text message or by sending picture messages using their mobile telephone or divulge their telephone number to pupils under any circumstances/unless given express permission by their line manager.

9.3 Employees provided with a mobile telephone to carry out their duties must ensure they only use the mobile telephone for the purposes agreed with their line manager. Any unauthorised usage must be reimbursed to the school and/or may be the subject of disciplinary action.

9.4 Any urgent phone calls or messages must be directed to the office who will notify employees immediately. Employees who need to use their mobile telephone to make or receive an urgent call during working hours must obtain prior authorisation from management to do so.

Children are not encouraged to bring mobile phones to school, and are only permitted to do so if there are extenuating circumstances such as after school care arrangements. In such cases, the child must declare that they have brought a phone into school and hand it in to the school office or class teacher for safekeeping during the school day

8. Supervising and Monitoring Usage

Staff will discuss objectives for internet use to teach pupils about e-safety.

Pupils will be taught effective use of the internet when researching material including skills in locating, retrieving and evaluating information.

Parents are also encouraged to use these 'best practices' when allowing their children to access the Internet at home.

While using the Internet at Messing Primary, pupils will be supervised. However, when appropriate to their age and their focus of study, pupils may pursue electronic research independent of staff supervision, this will be at the discretion of the teacher in charge. In all cases pupils will be reminded of their responsibility to use these resources in line with the school policy on Acceptable Use as detailed in this policy document. (Appendix B and C)

9. Handling e-safety Complaints

Complaints of a Child Protection nature will be dealt with in accordance with school child protection procedures and reported to the Head teacher.

This policy will be monitored by the Computing Subject Leader, Headteacher, governors and will be reviewed in two years.

All staff are required to accept and sign the 'Acceptable use of the internet' agreement. (Appendix A)

Appendix A

Messing Primary School
Every Child | Every Chance | Every Day

Acceptable Use Agreement

How staff use school ICT

School ICT equipment, including the intranet, should be used for school related purposes. Personal use is accepted on the provision usage is in accordance with this agreement, the e-safety policy and deemed reasonable by the headteacher.

When ICT equipment is to be used staff members must arrange this prior to the lesson and notify each other.

County guidance is that laptops are not to be left in cars unattended.

Child safety

It is our responsibility to educate and support our pupils to use electronic devices and the internet safely. We also have a responsibility to report to the e-safety officer (Headteacher) any e-safety issues which will be followed up and acted upon.

Social Networking

Access to social networking sites using the school's computer network is not permitted. Any access to social networking sites using mobile phones is restricted to break times/lunchtimes in the staff room only.

School related business is **not** to be discussed using social networking; this includes 'private' or 'direct messaging'. As a member of the school community we have a responsibility for upholding the Code of Conduct, which states use of social networking must not adversely affect the reputation of the school or bring the school into disrepute.

Befriending of pupils and ex-pupils from our school on social networking sites is not to be accepted. Befriending of parents is acceptable **but discussions of school related business or posting any comments or actions that could reflect on the school is not acceptable.**

Email

All emails involving school business are to be sent and received using the allocated school email address.

Audio, video and photography

Audio, video and photographic files remain the property of the school at all times. These are to be stored on google drive, icloud or mobile devices (iPad, cameras). These types of files are to be used for school related business; they can be taken and used off site but you are responsible for safeguarding the files and minimising risks.

Only school equipment is to be used for recording audio, video or photographic files. In exceptional circumstances and with the permission of the Headteacher. Personal equipment may be used. All data must be deleted once uploaded to the school system. You are able to use personal equipment to edit, manipulate and produce resources for these file types but you are responsible for safeguarding the files and minimising risks.

File sharing

File sharing, including the use of removable devices (memory sticks) and cloud based technologies (e.g DropBox) is the responsibility of the user to safeguard the information being used and minimise risks.

Personal Devices

Personal devices such as mobile phones, tablet computers and laptops should not be used for personal use other than in staff areas e.g. staffroom during your own time. Personal tablets and laptops can be used for educational purposes but you must ensure that they are free from virus and malware which cannot be transferred to our school system. Please refer to the above section regarding audio, video and photography.

GDPR data protection requirements are adhered to as is the staff code of conduct.

If you have any queries, are unsure of anything, or do not have a definitive answer for, please seek advice from the headteacher before proceeding.

Any breaches of this agreement could lead to disciplinary action under the school's disciplinary procedure, including dismissal in serious cases.

I have read and understood the 'Messing Primary School Acceptable Personal Use of Resources and Assets Policy.'
I confirm that I have read and understood the above.

Signed ……. Date ……..

Name (please print)……...

Appendix B

Messing Primary School

Responsible Internet and Computer Use Agreement
Foundation / KS1

In order to keep ourselves and others safe I agree to the following:

1. I will ask an adult if I want to use the computers or ipad.
2. I will only use activities that an adult has allowed me to use.
3. I will take care of the computer and other equipment.
4. I will ask for help from an adult if I am not sure what to do or if I think I have made a mistake.
5. I will tell an adult if I see something that upsets me on screen.
6. I know that if I break the rules I might not be allowed to use a computer or tablet.
7. I will not put into the internet any facts about myself or my house or my school.
8. I will not download any files, apps or games on the iPads or laptops, unless I have been asked to by an adult.

Appendix c

Messing Primary School

Responsible Internet and Computer Use Agreement KS2

In order to keep ourselves and others safe I agree to the following:

1. I will use the school computers, Internet, and all our technological equipment sensibly.

2. I will not enter chat rooms or leave messages on bulletin boards.

3. If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

4. I will never insert my personal details, home address, or telephone numbers on the Internet or in an e-mail.

5. I will only e-mail people or open e-mails from people I know, or my teacher has approved.

6. I will always be polite and use appropriate language when sending e-mails.

7. I will not look at or delete other people's files without their permission.

8. I will only use my own username and password to access learning websites.

9. I know that the school may check my computer files, monitor the Internet sites I visit and filter the contents of my e-mails.

10. I will not download any files, apps or games on the iPads or laptops, unless I have been asked to by an adult.

11. I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.