High March

E-Safety Policy

Person responsible for latest revision:	Mrs J Halford and Mr M Wright
Page number of any significant changes in latest revision:	
Date of next review:	February 2025

ISI Reference	7h

This policy applies to the Early Year Foundation Stage, Key Stage 1 and Key Stage 2

Useful Websites	
www.education.gov.uk	www.kidsmart.org.uk
www.childnet.com	www.lgfl.net/online-safety
www.thinkuknow.co.uk	www.swgfl.org.uk/resources
www.teachcomputing.org/curriculum	www.gooseberryplanet.com

High March

E-Safety Policy

Introduction

At High March School we use technology and the Internet extensively across all areas of the curriculum and as such safeguarding and applying appropriate controls/restrictions are essential. Online safeguarding (E-Safety) is an area that is constantly evolving and as such this policy will be reviewed at least annually by the SLT. The Designated Safeguarding Lead reports annually to the Governing Board on online safety, filtering and monitoring as part of her annual Safeguarding Report to Governors.

The primary purposes of this policy are:

- To empower the whole school community with the knowledge to stay safe and reduce risk.
- To ensure that risks are clearly identified, assessed and mitigated in order to reduce any potential harm to pupils and staff, and any liability for the school.

This document provides a guide for adults working in our School about acceptable and desirable conduct to protect both adults and pupils. It also includes guidance for pupils and parents on E-Safety issues. It refers to and complements other policies and guidance at High March School with which all staff, volunteers and visitors must be familiar and work in accordance with. The policies include:

- Child Protection Policy
  ISI 7a High March Child Protection and Safeguarding Policy
- Staff Code of Conduct
  ISI 7e High March Code of Conduct for Staff
- Behaviour Policy
  ISI 9a 15a Behaviour and Pastoral Care Policy
- Acceptable Use of ICT Systems Policy and Internet Safety
  HM ICT Security Policy
- Anti-Bullying Policy
  ISI 10a Anti-Bullying Policy
- Equal Opportunities Policies
  ISI 17a Equal Opportunities for Staff
  ISI 17a Equal Opportunities for Pupils Parents
- Health and Safety
  ISI 11 Health and Safety Policy

- Staff Handbook
  Staff Handbook

- Guidance on Photography and Recording images of pupils
  ISI 7a i Mobile Phones and Images Policy

- Mobile Phone Guidance
  ISI 7a i Mobile Phones and Images Policy

- Data Privacy Notices
  Data Privacy Notice for Parents
  Data Privacy Notice for Pupils
  Data Privacy Notice for Staff

All the above policies can be found in the Policies Channel of the Whole School Staff Team in Microsoft Team and on the School website.

You should also be aware of the following documents:

- Keeping Children Safe in Education 2023
  All staff should read, understand and comply with their roles and responsibilities laid out in Part 1 and Annex A

- Working Together to Safeguard Children 2023

- What to do if you're worried a child is being abused 2015

It is the aim of the School to ensure that staff/adults do not place themselves in situations of vulnerability in their professional duties. To help staff/adults in this we would advise that the points in this document are heeded. This list is not intended to be definitive, and we understand that professional judgment will be needed in dealing with situations that arise.

1. Teaching and Support Staff

All adults working in our School should know the name of the Designated Safeguarding Lead (DSL) and the Deputy Designated Safeguarding Leads (DDSL) and the Designated Safeguarding Governor be familiar with our Child Protection Policy and understand their responsibilities to safeguard and protect children and young people.

All staff should be aware of the school policies and documents on E-Safety, available in the Whole School Staff Team, which set out our expectations relating to:

- Creating a safer online environment.

- Giving everyone the skills, knowledge and understanding to help children and young people stay safe online.

- Inspiring safe and responsible use and behaviour.

- Use of mobile phones both within school and on school trips/outings.

- Use of camera equipment, including camera phones.
- What steps to take if you have concerns and where to go for help.
- Staff use of social media as set out in the Staff Code of Conduct and ICT Acceptable Use Agreement. *GSWP Sept 2019 (Guidance for Safe Working Practices for the Protection of Children and Staff)*

The E-Safety Officer, who is also the Network Manager, will:

- Familiarise himself with the latest research and available resources for school and home use.
- Assist the DSL and DDSLs in keeping up to date with the latest risks to children using technology.
- Review this policy regularly (in conjunction with the Head of Computing) and bring any matters to the attention of the Senior Leadership Team (SLT).
- Advise the SLT and Directors on all significant E-Safety matters.
- Along with the Head of Computing, engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the E-Safety incident log and ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical E-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make himself aware of any reporting function with technical E-Safety measures (e.g. Internet filtering reporting function).
- Ensure that anti-virus software is fit-for-purpose, up to date and applied to all capable devices.
- Ensure that operating system and software updates are regularly monitored and devices updated as appropriate.
- Ensure that any E-Safety technical solutions, such as Internet filtering, are operating correctly and have been applied correctly.
- Ensure that passwords are applied correctly to all users.
- Ensure that the network administrator password is changed regularly.

All staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headmistress.
- Any E-Safety incident is reported to the E-Safety Officer as soon as possible, and certainly within 24 hours, so that appropriate action can be taken. If staff are unsure, the matter should be raised with the E-Safety Officer who will make appropriate decisions.

2. Pupils

- The boundaries of use of ICT equipment and services in School are given in many ways, including the Responsible Use Policy and the Behaviour Policy.
- All pupils in Years 3 – 6 are asked to sign and agree to the Responsible Use Policy every September.
- Any deviation or misuse of ICT equipment or services, including misuse of online chat and/or social media. will be dealt with in accordance with the School Behaviour Policy, where necessary.
- It is the School's aim for E-Safety to be embedded into the curriculum – pupils will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- All Year 3 – 6 pupils will be made fully aware of how they can report E-Safety concerns whilst at school or home.

3. Parents/Carers

- All parents/carers should be aware of the School policies and documents on E-safety, available on highmarch.co.uk/our-school/school-policies.
- Parents play the most important role in the development of their children and, as such, the School will support parents in accessing resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment.
- Through parent information evenings, school newsletters and the availability of free online training courses (e.g. Think U Know) the School will seek to make parents aware of new and emerging E-Safety risks.
- Parents must also understand the School needs to have rules in place to ensure that their child can be properly safeguarded. As such all parents will sign the Responsible Use Policy.

4. Network and Device Management

High March School uses a range of devices including desktop PCs, laptops and tablets. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

The School uses a web content filter that prevents unauthorised access to illegal websites and inappropriate websites. The E-Safety Officer is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headmistress.

Email Filtering

The School uses Microsoft Office 365, which contains facilities to help protect staff and pupils from infected emails. Infected is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data, a spam email such as a phishing message, etc.

Network Monitoring

The School uses a number of tools to monitor network usage. Principal amongst these is Impero Education Pro, which monitors key presses and produces real-time alerts if certain key safeguarding trigger words or phrases are typed. Staff are also able to use Impero to monitor their class while using laptops or workstations (but not tablets) and to perform functions such as locking computers, sending a web link to all computers at once, etc.

Passwords

Staff and pupils will be unable to access any critical part of the School network without a unique username and password. Staff and pupil passwords should be changed if there is a suspicion that they have been compromised. Staff are prompted annually to change their network passwords. The Head of Computing and Network Manager will be responsible for ensuring that pupil passwords are changed as and when required.

Anti-Virus

All capable devices have anti-virus software. This software is updated multiple times each day with new virus definitions. The E-Safety Officer is responsible for ensuring this process is not compromised.

5. Email

All School employees are issued with a School email account, an address ending with:

@highmarch.co.uk

All staff are reminded that emails are subject to Freedom of Information or Data Subject Access Requests and, as such, the email service is intended to be used for professional work-based emails. The use of email (work or personal) for the purposes of contacting pupils is not permitted.

Pupils in Years 3 – 6 are permitted to use the School email system as part of their online learning and, as such, are all issued with a High March email account and their own approved email addresses. Pupil email addresses are sometimes disabled for entire year groups when not in use (e.g. in school holidays.) Pupils should use their email account only for school-based activity as laid out in the Responsible Use Policy.

6. Photos and Videos

All parents receive guidance on photography or recording of images of High March pupils. A list of pupils whose parents have indicated that they would not like their child's image published will be held by the School Office.

Pupils may not take photos or video footage for personal use anywhere on the School site, including during remote learning. Any photos or video footage taken in lessons (to enhance a practical activity, etc.) must be deleted once their purpose has been fulfilled.

Photographs with names directly identifying the pupil will only be published by the School in line with the terms of our Privacy Notice for Pupils and Parents.

7. Social Networking

Any use of social media services in School must be in accordance with the

- ICT Acceptable Use Agreement (for staff)
- Responsible Use Policy (for pupils)
- Privacy Notices for Staff, Parents and Pupils

8. Copyright

Should it be brought to the School's attention that there is a resource that has been inadvertently uploaded, either to the School website or school/department authorised social networking sites, and the School does not have copyright permission to use that resource, it will be removed within one working day.

9. Reporting E-Safety Incidents

Any E-Safety incident must be brought to the immediate attention of the E-Safety Officer and /or the Data Protection Officer (DPO). The E-Safety Officer will assist in taking the appropriate action to deal with the incident, liaise closely with the relevant staff, including the DSL, to ensure the appropriate resolution of the incident and complete and maintain any necessary documentation. All staff should make themselves aware of the procedures and the responsible staff involved in the process.

10. Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology. This includes updated awareness of new and emerging issues, and the regular distribution of E-Safety information to staff, pupils and parents. The School will aim to ensure that aspects of E-Safety for pupils are firmly embedded into the curriculum. Whenever ICT is used in School, staff will encourage pupils on the safe use of technology and risks, as appropriate, as part of the pupils' learning and understanding.