Marshfields School E-Safety Policy

E-Safety Staff Co-ordinators: Hannah Mills (curriculum) / Paula Elton (pastoral)
E-Safety Senior Lead: Janet James.
E- Safety Governor: Amanda Walls

Publication Date: May 2018

This policy is monitored by the governing body and will be reviewed every two years, or earlier if necessary.

Introduction

The e-safety policy is part of the school development plan and relates to other policies, including those for computing, anti-bullying and Child Protection.

The internet is an essential resource in 21st century teaching and learning. Internet use is a statutory part of the curriculum and a necessary tool for both staff and students. Through the use of school PC's, laptops and tablets students currently access the internet via websites, emailing, blogging, gaming, learning platforms and Google Apps for Education.

Any personal data will be recorded transferred and made available according to the Data Protection Act 1998 and the GDPR May 2018

Teaching and Learning

The school internet networks will be:

- Designed specifically for student use,
- Include internal filtering System, Lightspeed and appropriate monitoring in conjunction with Peterborough Local Authority and E2BN.
- Follow an acceptable use policy for both staff and students (appendix 2),
- Used to publish and present information where appropriate and in line with this policy,
- Ensure staff are aware of their responsibility to report any unsuitable online materials that are accessible to students immediately as they are aware of them.

Students will be taught:

- How to effectively use the internet for research, including skills of knowledge location, retrieval and evaluation.
- Acceptable and unacceptable usage of the internet as laid out in appendix 1 and through national e-safety standards.
- How to ensure that their use of the internet complies with copyright law and how to acknowledge sources of information in line with these laws and guidelines.
- How to report unacceptable internet content and user behaviour to staff and through CEOP.
- Awareness of dangers online relating to grooming, CSE and risk of radicalisation and how to report any such risk they encounter.
- The above skills and knowledge will be embedded across the school curriculum along with being taught explicitly in Computing lessons and through participation in whole school and national initiatives based around e-safety such as National Safer Internet Day.

Managing Internet Access

Information system security

- All staff and student user logins and details not to be shared.
- When users leave a station/device they should either logout or click the lock button.
- School ICT systems and security will be reviewed regularly in line with guidance from the Local Authority.

Email

- Students may only use approved e-mail accounts on the school system - these are their Microsoft Office 365 and Google Apps Gmail accounts.
- These accounts may not be used to sign up for personal sites such as social media and gaming outside of those directed by teachers and/or the leadership team.
- Students Gmail accounts are to be monitored regularly by the curriculum e-safety co-ordinator.
- Students must report any suspicious or inappropriate behaviour or contact to a member of staff immediately.
- Staff have a duty to ensure that emails to external bodies (including those sent by students) are presented in a considered way.
- Users (staff and students) must not send jokes or material others may find offensive.
- The school email systems are not to be used by staff or students as personal email accounts.

Published content and the school website

- The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.
- The head teacher and SLT will take overall editorial responsibility and ensure that website content is accurate and appropriate.
- The CEOP button will be shown on both the school website homepage and the e-safety page in the Computing curriculum area of the site.
- Photographs of students will be selected carefully so that images cannot be misused.
- Images of students will not be published on any public spaces such as staff social media or shared via staff personal email/instant messaging accounts.
- Staff will be made aware of the list of students whose parents/guardians have NOT given permission for their child's images to be published and where this list can be accessed centrally.
- Students full names will not be published anywhere on the school website or other public online spaces, particularly in association with photographs.
- Images of students should not be taken on personal devices such as phones and/or tablets.
- Parents will be clearly informed of the school policy on image taking and publishing.

Social Media and personal devices

- The school will control access to social networking sites via Lightspeed filters and educate students in their safe and positive use.
- Students and parents will be advised that the use of networking spaces outside school brings carries a range of risks and dangers to all students, especially those with more complex needs.
- Students will be advised that the use of nicknames and avatars can aid in minimising risks.
- Users will also be taught through the Computing curriculum within school about the impact of social media on reputation and the impact of this in employment and further education upon leaving Marshfields.
- Students will be advised on how to evaluate images they are posting on social media as to whether they give away personal information that could put them at risk (e.g. a school jumper, street sign where they live etc.)
- Should the school become aware of any form of cyber-bullying/trolling incidents by any students inside or outside school will be dealt with according to the school behaviour policy and parents informed and met with where necessary by the pastoral e-safety co-ordinator .

- Students and staff will be made aware that they should never give out personal details that may identify themselves, their location or their friends/associates.
- All students are required to hand in any electronic devices at the beginning of each school day to their tutor team, these are then kept securely in the school office until students leave for the day. Students found to be carrying electronic devices/accessing the internet via an electronic device that should have been handed in will be dealt with in line with the school behaviour policy.
- Staff are not to give students or parents/carers their personal mobile phone or email addresses. Where a pre-existing relationship with a parent/carer exists staff should ensure that senior leadership are made aware of this and of the nature of the relationship.

Managing emerging technologies

- Emerging technologies, in particular software, will be examined for educational benefit and risks with permission for use to be then sought from senior leadership before implementation.
- Senior leadership should be aware that constant new developments with devices such as mobile phones, handheld gaming devices and headphones/sets with wireless internet capabilities means students can be use these to bypass school filters and security.

Monitoring & Authorisation

Monitoring

- The IT technician will provide weekly reports to the head teacher on staff and student internet usage.
- The head teacher has the right at any point to request a full report on any student or member of staff's internet usage on school site.
- Staff who suspect a student is misusing the internet inside school should report this immediately to the curriculum e-safety coordinator or if they suspect it is happening outside school to the pastoral e-safety co-ordinator in line with Prevent.
- All staff through Prevent training will be aware of the Counter Terrorism abd Security Act, 1st July 2015 in particular that the school have a duty to "have due regard to the need to prevent people being drawn into terrorism".
- Staff who suspect a student is misusing the internet inside school should or outside school in a way that puts themselves or others at risk should report their concerns to the designated safeguarding lead following the school's safeguarding procedures.
- Any complaint about staff misuse must be reported to a member of the senior leadership team

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Student misuse will be dealt with according to the school behaviour policy as set out above.

Assessing risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never be displayed/accessed on a device connected to the school network, Neither the school nor PCC can accept liability for any material accessed, or any consequences of internet access.

Appendix 1 – Student Guidance

S Successful
H Happy
A Aspiring
P Purposeful
E Exciting
D Diverse

Stay Safe

Being Smart and Safe On the Internet?

- ☐ I will have an adult present when I use the internet.
- ☐ I will only use the websites and do searches that my teacher asks me to.
- ☐ I will only use my own login and save work in my folders.
- ☐ I will keep my password a secret.
- ☐ Files I save and messages I send will be polite, sensible and not upset anyone.
- ☐ I will not open emails or attachments from someone I don't know.
- ☐ I will never give out my personal details; full name, home address or telephone number.
- ☐ If I see anything I am unhappy or uncomfortable with I will tell an adult immediately.
- ☐ If I see anything I know is inappropriate I will tell an adult immediately.
- ☐ The school are allowed to check my files, internet use and school email account.