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 2016

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

Teaching and Learning

The school internet networks will be:

- Designed specifically for student use,
- Include filtering 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 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.

Appendix 2 - MARSHFIELDS SCHOOL – ICT ACCEPTABLE USE POLICY

Refer to

- INFORMATION, COMMUNICATIONS AND TELECOMS (ICT) POLICY OF PETERBOROUGH CITY COUNCIL
- DISCIPLINARY POLICY – MARSHFIELDS SCHOOL
- EQUAL OPPORTUNITIES POLICY - MARSHFIELDS SCHOOL
- 1988 DATA PROTECTION ACT
- 1959 OBSCENE PUBLICATIONS ACT
- 1978 CHILDREN'S ACT
- 2000 FREEDOM OF INFORMATION ACT
- MARSHFIELDS SCHOOL E-SAFETY POLICY 2015

Introduction

The policy relates to use of:

- Email
- Internet facilities
- Access to/use of the school's Wi-Fi network
- Devices (e.g., tablets/phones, etc.)

It also applies to:

- Items provided by the School, or personal items of members of staff, whether or not connected to the School's Wi-Fi/internet connection.

This policy outlines the duties and responsibilities of employees whilst using equipment or facilities provided by Marshfields School. This includes access to the school's network and wifi-system. Whilst these facilities are made available to users for business purposes related to Marshfields School, a certain amount of limited and responsible personal use is permitted, although the School reserves the right to withdraw this permission for personal use from an individual, group or whole staff at any time.

Staff are responsible for reading and understanding the policy and keeping up-to-date with any amendments. Ignorance of the policy is not deemed an excuse for not following the guidance contained in it.

Failure to comply with the policy could result in disciplinary action under the disciplinary policy and ultimately result in an employee being dismissed. Incidents of misuse will investigated/actioned under the School's Disciplinary Policy, but staff should be aware that it may be necessary to report incidents or provide relevant information to the Police for criminal investigation.

Generally

1. Employees must use the facilities sensibly, professionally, lawfully and consistently with their duties. In doing so, they must treat colleagues and clients with respect and have regard for other relevant policies, such as Equal Opportunities and E-Safety. Any material disseminated which is discriminatory or encourages discrimination may be unlawful. Staff must not create and/or distribute any text or material likely to cause annoyance, inconvenience or needless anxiety, either by deliberate design or intent, or not. They also have a duty to ensure that anything created/transmitted is not abusive or threatening and neither serves to harass or bully others, i.e., defamatory information/material. This would include materials which discriminate (or encourages discrimination) on the grounds of race, ethnicity, gender, sexual orientation, marital status, disability, political/religious beliefs or age.
2. All information received or distributed in relation to the School's business must be regarded as confidential and employees have a duty of care to ensure it remains so. Staff should not routinely forward/publish text written one-to-one to others without the permission of the original author. Neither should staff amend messages without permission of the original author. Usernames and passwords should be kept secure and regularly updated to maintain security levels. Any equipment/device used in relation to Marshfields/local authority business, whether or not owned by the School, must be password protected. Staff must guard against information being displayed inappropriately, e.g., by leaving confidential information on a printer accessed by multiple users or failing to lock the computer screen when leaving the equipment unattended (regardless of the length of the time period involved). When working remotely (eg, at home), staff must also ensure confidentiality, legal use and application of this policy when undertaking work related to Marshfields School or the local authority.
3. Staff should be aware that the downloading, copying, possessing and distribution of material from the internet may be an infringement of copyright or intellectual property rights for which the School may become liable. Putting this School into this position would be deemed a disciplinary matter for the employee. However, there are instances where the law has a general "fair dealing" exception, allowing copying of works in any medium as long as the following conditions apply:
    a. The work must be used solely to illustrate a point;
    b. The use of the work must not be for commercial purposes;
    c. The use must be fair dealing; and
    d. It must be accompanied by a sufficient acknowledgement.

    A criminal offence is committed if a person publishes any material which is pornographic, violent or which comes under the provision of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child/ren and if any such material is discovered on Marshfields' equipment, the matter will be referred directly to the police. The intention or action of searching for/downloading such material would initiate a disciplinary investigation which may also lead to the police being informed. Similarly staff must not create or transmit offensive, obscene or indecent images/material, or any data capable of being manipulated into an obscene or indecent image/material.
4. Employees are made aware that the legislation relating to libel applies whether the action has been made during, before or after work hours. This is where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation (including Marshfields School, staff or clients, past or present) will rest mainly with the sender of the information and may lead to substantial financial penalties being imposed, as well as be the cause of disciplinary action being taken against that individual or group.
5. Staff are made aware that expressions of fact, intention or opinion in any email may bind the employee/Marshfields School and can be produced in court alongside other kinds of written documents.
6. Staff are also advised that they should be aware to consider the content of all electronic information sent prior to despatch to ensure the message could not be described as "ill-considered". Line managers can provide oversight and advice in these instances. Staff are advised to re-read messages prior to sending.
7. Employees must comply with the Data Protection and Freedom of Information legislation.
8. Staff must guard against information being made available to known/unknown parties in a way that would be considered, "unauthorised". For example, sending personal information about a student by unencrypted email.
9. Anonymous messages are not allowed. Neither is the transmission of information which might be considered to bring Marshfields School into disrepute.
10. Staff should avoid routinely using the CC function on emails where this could inadvertently mean that personal/confidential information, such as an individual's email address will be distributed to others instead using the BCC function.
11. Legal documents may not be transmitted by email.
12. Attachments to emails are considered under the same procedures above in relation to acceptable/unacceptable content. However staff should also be aware that due to the security risk posed, business communications should never be sent to email accounts not provided by the School or local authority, for example, Hotmail, Yahoo, etc.
13. School facilities, including email, must not be in connection with the operation/management of any business or private work except that of Marshfields School and the local authority. In addition, school email accounts may not be given for non-business use, e.g., for the purpose of personal internet shopping, social media accounts, etc.
14. Any use of the schools facilities/services must not be deemed to have taken priority over your normal duties and must not interfere with your performance or role and should be undertaken during unpaid breaks and must not result in any unwarranted expenditure or liability incurred by Marshfields School or the local authority.
15. Staff are made aware that the School has monitoring facilities in place for all aspects of ICT and that individual accounts, such as email accounts, may be routinely inspected as part of the School's overall policy to keep staff and students safe. All use of the School's facilities, including those which link to personal devices will be subject to the

School's monitoring procedures which will necessarily gather and store information of internet usage. Staff may not use personal devices on site for work purposes unless these have been recorded by our ICT support service, Innovit. Whilst it is permitted to do so, the School does not promote or support any notion that staff should/need to use personal devices for business purposes. If staff do not wish their personal devices to be monitored in this way, they must see our ICT support provider to have their device removed from the School Wi-Fi/internet system.

16. Where staff are using USB storage devices these should be checked by the onsite Innovit IT technician for risks such as malware, viruses, etc. before being plugged into any device connected to the school network.
17. Staff may not introduce to/modify equipment on the School's network/internet/Wi-Fi systems, including that which might detect passwords, unauthorised/personal software; nor undertake activities deemed to introduce/distribute a computer virus; nor carry out hacking activities. Such activities would be subject to disciplinary action being taken against the employee.
18. Where staff are issued with School equipment that is permitted to be taken off-site, the staff member has a duty to do all that is reasonably possible to ensure its safe and secure.
19. Staff must ensure their usage complies with all the Acts (and their updates) listed at the top of this policy.

Written by J James

Reviewed and adopted by Full Governor Committee
May 12th 2016

I…….. have read, understand and agree to adhere by the ICT Acceptable use Policy.

Signed……..

Dated…….

Please detach and return this signed agreement to the School Office as soon as possible.

Thank you