E-SAFETY & MEDIA POLICY

Original Policy: December 2012

Date Reviewed: December 2014, March 2015, September 2018

Media Policy

Policy Statement

The purpose of this policy is to:

- Ensure the governing body maintains its duty to safeguard children (KCSiE September 2018), the reputation of the School and wider community.

- Maintain appropriate professional boundaries in accordance with the Code of Conduct document and Staff Handbook.

- Safeguard pupils and staff and ensure that they do not make themselves vulnerable through new technologies either in school or at home.

1. INTERNET

1.1 The primary use of the Internet during working hours is as an educational tool, support tool or used for work purposes by staff.

1.2 Private use of the Internet will not be allowed other than for work-related purposes (i.e.; research whilst studying for exams CPD) or during breaks. This will be entirely at the discretion of their line manager.

1.4 Staff need to be aware that internet use can be and is monitored and that any excessive and/or inappropriate use may be the subject of disciplinary action.

1.5 E-mail is not private – it can be copied or forwarded. You may delete it, but it could still reside elsewhere and may later be accessed and read.

1.6 Computer Security – it is your responsibility to ensure security where this is necessary. You must keep your password confidential unless using a shared facility. Passwords must never be disclosed to unauthorised individuals or outside the School. Certain information within the School (notably pupil & staff records, finances and payroll) must be password protected at all times and individuals with this level of access must not allow access to any staff not entitled to this information. When leaving your workstation pressing the Windows Key and L will quickly secure your machine.

1.7 E-mail: any correspondence entered into can be classed as a contract and could be used in any legal action against you or the School

1.8 **DO NOT** access e-mail of any other employee unless specifically authorised.

1.9 **DO NOT** send e-mails from another employee's computer unless specifically authorised.

1.10 All information processed on the School's system is the property of the Marchant Holliday School, and may be accessed or monitored by the School.

1.11 Any employee that becomes aware of misuse should report this to their line manager as soon as possible.

1.12 On-line Safeguarding taken from KCSiE update September 2018

Mobile phones, laptops, iPads, and other on-line type products are integrated into all our lives. However, there are those that seek to use these for their own or others gratification. The link below provides more information on on-line safety and cover issues such as:

- Bullying, including online bullying and prejudice-based bullying, racialization and/or extremist behaviour
- Child sexual exploitation and trafficking
- The impact of new technologies on sexual behaviour, for example sexting.

The use of technology has become a significant component of many safeguarding issues, for example, technology often provides the platform that facilitates child sexual exploitation, radicalisation and sexual predation.

There are three categories of risk:

Content: being exposed to illegal, inappropriate or harmful material, for example, pornography, fake news, racist or radical and extremist views;

Contact: being exposed to harmful online interaction with other users, for example, commercial advertising as well as adults posing as children or young adults; and

Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images, or online bullying.

The governing body has had due regard to the additional information and support set out in KCSIE 2018 and will ensure that the school has a whole school approach to online safety and has a clear policy on use of communications technology in school.

http://swgfl.org.uk/news/News/E-Safety/Making-Sense-of-the-New-Online-Safety-Standards

Via e-Learning and Information Management (eLIM) and the SSCB and the South West Grid for Learning, will consider any improper use as a possible safeguarding concern, which should be considered as child protection issues and discussed with your line manager or DSL as appropriate.

2. PHOTOGRAPHY

2.1 Photography including use of video must only be undertaken with parental permission and for the purposes of recording school processes (i.e.; such as achievements, reports and school publicity).

2.2 School cameras must always be used for any recording.

2.3 Staff must not at any time use their personal recording devices (cameras, mobile phones, etc.) to photograph the pupils.

2.4 Staff must not publish images of any individual (pupil or staff) unless consent has been given in writing, using an official photograph consent form.

3. MOBILE PHONES AND LANDLINES

3.1 Staff are not permitted to give any pupils or ex-pupils their personal contact details. This includes telephone numbers, home addresses or e-mail addresses. Staff should not use personal phones to contact parents or carers.

4. SOCIAL MEDIA

4.1 What is Social Media?

'Social media' is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. Examples of social media websites include:

- Social networking (e.g. www.facebook.com)
- Transient message sites (e.g. www.instagram.com)
- Video sharing (e.g. www.youtube.com)
- Blogs (e.g. www.london2012.com/blog)
- Micro-blogging (e.g. www.twitter.com)
- Message boards (e.g. http://forums.moneysavingexpert.com)
- Wikis (e.g. www.wikipedia.org)
- Social bookmarking (e.g. www.delicious.com)

4.2

Outside of the School however, any individual can freely access social media sites from home, mobile 'phones or public internet facilities (cafes, libraries, etc.). This 'outside-of-work' access needs to be handled in a sensible and considered way so that neither the individual(s) involved nor the School is put at potential risk of embarrassment, loss, disciplinary action or criminal proceedings.

4.3 Scope

This guidance applies to all school employees, volunteers, governors and any persons working at the school. The guidance aims to raise awareness of the implications of using social media, by individuals having some role within the School, and it provides a framework for making responsible decisions about getting the most out of social media tools. (For information and resources see http://www.thinkuknow.co.uk).

Personal use of social media

4.4 When using third-party websites (such as Facebook, Instagram etc.), know and follow the terms and conditions of use.

4.5 Understand how to implement privacy tools, i.e.; only allowing known people to access information about you / see the content of your site. The more personal information you put on the site the more vulnerable you are to identity fraud

4.6 Never publish or disclose any information about the School which is not already in the public arena (usually defined as that material which is on the School's website). Be mindful that whatever you publish may be in the public arena for the long term and that doing so may result in disciplinary action being taken against you.

4.7 Do not publish or report on conversations that are meant to be private or internal to the School. Do not cite or reference pupils, ex- pupils, staff, parents/carers, other associated bodies, partners or suppliers.

4.8 Ensure that your online activities do not interfere with your job, your colleagues or commitments to pupils.

4.9 Do not befriend pupils, ex-pupils or their parents/carers or anyone you have to maintain a professional relationship with or individuals you support.

4.10 Do not under any circumstances enter into communication or correspondence with any pupils or former pupils under the age of 18, or with the parents/carers of any such pupils. This includes any contact whether by way of e-mail, electronic message facilities, and SMS text messages, telephone, Skype or other such media. Specifically, do not establish contact or allow any individuals within these groups to have access to your personal media site(s) or establish them as contacts in any way (i.e.; Facebook 'friends'). Any approaches from pupils/ex-pupils should be declined but advised promptly to your line manager.

4.11 Posting your feelings or inappropriate and unguarded comments can give you or the school a very negative image. Seemingly benign comments which may be routine within the workplace can assume much greater magnitude when published on social media sites and easily lead to a poor impression of the School and those who work for it. Negative comments posted by members of staff may well lead to disciplinary action by the school.

4.12 It is very easy to damage your own reputation so be careful. Pictures of that recent lively social event may be great to share between friends but what image of you do they represent professionally if ever taken out of context?

4.13 Do not use social media to discuss colleagues, pupils or anyone in connection with work. Respect the privacy, feelings, reputation and position of others you work with. Any such action may result in disciplinary action.

4.14 Do not include contact details or pictures of other staff members without their permission.

4.15 Staff should maintain boundaries between their personal and professional lives by customising their privacy settings and avoiding inappropriate personal information becoming visible.

Respect your audience. Do not publish anything that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered controversial or invoke a bias, such as politics and religion.

4.16 **Commenting on news feeds/articles.** Many websites, particularly news sites, invite comments or have a 'chat thread'. Such sites have to obey House Rules and use pen names rather than actual names of contributors.

E-Safety

General statement of E-safety

Due to the proliferation of broadband, children are growing up in a world where electronic communication is ever more widespread and normalised. As a consequence, it is vital that children are made aware of the risks, dangers and potential hazards concomitant with this increase in electronic communication. At the Marchant Holliday School, pupils are taught about the risks involved with chat-rooms, online stranger danger and cyber-bullying associated with all forms of electronic communication.
These are taught through the heading of 'E-safety skills'. This covers all aspects of E-mail and how to e-communicate safely and how to identify potentially dangerous E-mails from unknown sources. It also addresses the potential problems associated with social networking websites and chat rooms. All pupils are taught how to identify the risks involved with such sites and how to ensure that they do not place themselves at risk from unreliable or untrustworthy online web users.

Pupils are always supervised when they are using the Internet and are prohibited from using social networking sites and chat rooms. Pupils do not have direct or uncensored access to E-mail. E-mails come in through a staff-authorized mailbox and both incoming and outgoing mail is monitored for E-safety. Provision for E-safety is further enhanced by using the most secure Internet browsers and by setting Web preferences to the highest levels of security. There is no general access for staff or pupils whilst at school. The school uses an external IT Management company, Prodigy, to manage accounts, Firewalls, filters, e-mail traffic and off site cloud storage https://www.prodigyitsolutions.com/

E-safety knowledge and understanding is covered not only in computing but through the PSHE curriculum, during class 'circle time' sessions and assemblies. Understanding of the importance of E-safety is strengthened by posters in the ICT suite and around school presenting reminders, furthermore, at all other times when the pupils are using ICT in other areas of the curriculum.
The school uses a range of resources through the Jigsaw PSHE package and the Thinkyouknow website which is related to CEOP:
https://www.thinkuknow.co.uk

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 management systems.

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries for example
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff

- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support
- Exchange of curriculum and administration data with partner LAs and DfE

How will Internet use enhance learning?

- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Manager Mr G Paul and the school's DSL Mr R Teasdale.
- Staff and pupils should ensure that their use and / or sharing of Internet derived materials complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How will e-mail be managed ensuring safety for pupils and staff?

- Pupils and staff may only use approved e-mail accounts on the school system. Pupils are taught how to compose and send e-mails but do not have e-mail use in school unless part of lessons and any other form of e-mail use must be agreed by the school
- Pupils must immediately tell a staff member if they receive offensive e-mail. Routine e-mail access is not available in school to pupils
- Staff must immediately tell a member of SMT if they receive offensive e-mail or complete e-safety log.
- Pupils must not reveal details of themselves or others in e-mail communication or via a personal web space, such as their age, the location of the school, messaging account details, an address or telephone number, or arrange to meet anyone.
- Personal e-mail or messaging between staff and pupils should not take place
- The forwarding of chain letters is not permitted

How should website content be managed?

- The point of contact on the website will be the school address, school e-mail and telephone number. Staff home information will not be published
- Website photographs will be carefully selected and will only show pupils whose parents/guardians have given permission for their photographs to be used
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs

- The School Finance Manager will take overall editorial responsibility for the website and ensure that content is accurate and appropriate

Newsgroups, e-mail lists and forums

- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted. Each class has its own Class News page on the school website. Photographic permissions and content are moderated by the School Finance Manager.

Chat and Instant Messaging

- Pupils will not be allowed access to public or unregulated chat rooms. The school is aware that many on-line games, even when age appropriate have chat room capability.
- Pupils will not access social networking sites for example 'Facebook' or 'Myspace'
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised
- Any form of bullying or harassment is strictly forbidden (see Anti-Bullying Policy)
- A risk assessment will be carried out before pupils are allowed to use a new technology in school the School Finance Manager and Head Teacher must be informed and consulted

Personal websites and blogs

- When publishing materials to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises, upsets/distresses or bullies someone else, or is otherwise offensive, is unacceptable

How can emerging ICT applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupil access to the Xbox or Wii will be in such a manner that access to on-line users is not possible through Web Filters.
- Pupil mobile phones are not be used during the school day. Any phone or device brought into school is stored securely in the taxi box until transport arrives again in the evening. Boarding pupils have access to incoming calls from parents and carers but do not have their own devices on site.
  -Pupil phones are to be handed to staff on arrival and will be kept until the pupil leaves for home.
  - Staff mobile phones are to be kept in the staff room or locked in cars, to be accessed during timetabled breaks or pre-approved use (i.e. trips)
- The sending of abusive or inappropriate text messaging is forbidden
- Mobile phone cameras should not be used and photographs should not be forwarded to unknown sources
- The use of blog messaging on social network sites is strictly forbidden

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly through our partnership with Prodigy IT Solutions and the Governing Body.
- Access is strictly forbidden to any websites that involve gambling, financial scams, pornography and adult material.

How will filtering be managed?

- The school will work in partnership with parents, the LEA and own staff to ensure systems to protect pupils are reviewed and improved. The school uses an external IT Management company, Prodigy, to manage accounts, Firewalls, web filters, e-mail traffic and off site cloud storage https://www.prodigyitsolutions.com
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the School Finance Manager, SMT or complete an e-safety log.
- SMT with our IT Provider on site and remotely, will ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk)

How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede internet access
- A module on responsible Internet use will be included in the PSHE and computing curriculum covering both home and school use. CEOP and ThinkYouKnow materials are used regularly in assembly and class.

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the ‘responsible Internet Use’ statement before using any internet resource in school
- All new staff will be taken through the key parts of this policy as part of their induction
- All staff including teachers, teaching assistants, care staff and support staff will be provided with the School e-Safety Policy and have its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible internet use, and on the school Internet policy will be provided as required
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security. The school uses an external IT Management company, Prodigy, to manage accounts, Firewalls, web filters, e-mail traffic and off site cloud storage https://www.prodigyitsolutions.com
- Virus protection will be installed and updated regularly
- Personal data sent over the internet will be encrypted or otherwise secured (Appendix 1)
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed and its content can be searched by a member of staff.
- Files held on the school network will be regularly checked

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Management Team
- Any complaint about staff misuse must be referred to the Head Teacher
- Pupils and parents will be informed of the complaint procedure (Complaints Policy on school website)
- Parents and pupils will need to work in partnership with staff to resolve issues
- There may be occasions when the police must be contacted. Early contact should be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the Responsible Internet Use Policy in communications, and on the school website
- Internet issues will be handled sensitively to inform parents without undue alarm
- A partnership approach will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home. The school website has external links to E-safety resources and advisory websites e.g. CEOP, ThinkYouKnow and Somerset LSCB.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents. In some instances school staff may visit the home to apply Web Filters at the request of the parent or carer.

RESPONSIBLE ICT USE POLICY

Rules for staff and students

The school owns the computer system, hardware and infrastructure and has responsibility for Broadband provision. This Responsible ICT Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

- Irresponsible use may result in the loss of internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- School computer and Internet use must be appropriate to the student's education or to staff professional activity
- Copyright and intellectual property rights must be respected
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and may be seen by unexpected recipients
- Users are responsible for any e-mail they send and for contacts made
- Anonymous messages and chain letters are not permitted
- The use of chat rooms is not allowed
- Staff to ensure pupils only have access to the computer system through the "pupil" specific logon.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes of for storing unauthorised or unlawful text, imagery or sound.

Appendix 1

E-Safety and GDPR

GDPR IN SCHOOL – general considerations:

1 SOFTWARE AND FIRMWARE
GDPR Article 32 1 (b) refers to the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. A comprehensive systems architecture assessment was undertaken in October 2018 with our provider Prodigy IT Solutions. https://www.prodigyitsolutions.com .
All hardware on site is documented – whether it is supported, when it is due to go end-of-life, and if it has all the correct software and firmware.

If it is end-of-life or out of support, then a risk assessment is completed to define the risk to integrity and security of data should you continue to use it – if the risk is deemed too high, then it will be replaced. If equipment is within support, but is not up-to-date with software patching, the school will implement processes and procedures to minimise the risk of this happening again.

2 DOCUMENTION OF THE SCHOOL ICT SYSTEM AND MANAGEMENT PROCESSES AND POLICIES
GDPR Article 32 1 (c) relates to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. Article 32 1 (d) describes processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The school's documented IT systems and processes, allow regular testing and evaluation the effectiveness of the technical and organisational measures required to ensure the security of processing data.

In the event of a system failure, all IT systems (and data these support) can be quickly and efficiently restored following a controlled and tested approach. A governance framework will be implemented to evidence this as well as regular external assessment to guarantee it.
We work alongside our managed service to ensure and quality review the documentation created by the managed service provider.

3 DEFINING AND COMMUNICATING THE PURPOSE FOR DATA PROCESSING

With the prevalence of multiple platforms, the school continually seeks to minimise the risk of uncontrolled propagation of personal data.

The school system is continually evaluated for in terms of data types so everyone understands what data should be stored where and for how long. For most school purposes this includes the P-Drive, or Public drive, and stored documents. Data Privacy Impact Assessments will be carried out on each system – and evaluate it for measures such as encryption and pseudonymisation

4 UNENCRYPTED PORTABLE STORAGE FOR TRANSFERRING DATA

Unencrypted portable storage for transferring data, presents a significant risk to data security. GDPR Article 32 (b), requires assessment of an appropriate level of security in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Appropriates technical and organisational measures in school (such as encryption) should always be used to protect identification of data subjects.

This should involve the use of encrypted data storage and transfer by USB devices or e-mail encryption (Article 32 and Article 5) which relates to the processing of personal data.

In the sharing of data with Somerset Council the school uses Egress Switch.
https://www.egress.com/

Through Microsoft Office 365 it is also possible to send secure encrypted data that requires the recipient to have a one-time passcode. This facility exists on the school network and Office 2016 package.

Microsoft Office 365 Message Encryption MicrosoftOffice365@messaging.microsoft.com

Last Updated September 2018