E-SAFETY

Policy Reference Number:	Issue Date: June 2020	Review Date: June 2021

General statement on E-Safety

Children grow up in a world with a variety of electronic communication devices and social media platforms. It is therefore vital that staff, children and parents & carers are aware of the associated risks and measures that follow in order to keep children safe.

At The Marchant-Holliday School, pupils are taught E-safety which covers key aspects of email usage, safe communication and how to identify potentially dangerous emails and messages from potentially unknown sources. E-safety also addresses the benefits of social networking websites and chat rooms but also, the associated risks. Pupils have their own secure computer login credentials.

In ICT/Computing lessons, pupils learn about:

- Personal information and how to keep it safe; including the name of the school, the address and the telephone number
- Cyber-bullying
- Phishing, spear-phishing and cat-phishing scams
- Fake emails and websites
- Unsafe internet use and behaviour and how to report it
- Chatbots
- Chat and instant messaging

Pupils are always supervised when they are using the internet and cannot access social networking sites and chat rooms due to web filtering. Pupils do not have direct access to email accounts.

E-safety is aided by using the most secure internet browsers and by setting web security preferences to the highest levels. The school uses an external IT management solutions company to manage its firewall, web filter, update software, store data and manage anti-virus software.

E-safety is covered not only in ICT and Computing lessons, but also through the PSHE curriculum, wider curriculum and assemblies. Understanding of the importance of E-safety is strengthened by posters linked to learning in the ICT suite. The school uses a range of resources through the commercial Jigsaw PSHE package and the **Thinkyouknow** website which is related to CEOP: **https://www.thinkuknow.co.uk**

A risk assessment is carried out before pupils use a new technology in school by a member of teaching staff and the Finance & ICT Manager.

The school also has two members of staff appointed as CEOP ambassadors who contribute to the professional development of staff.

Internet

The purpose of the internet in school is to support pupil achievement; building knowledge, awareness and understanding and to support the professional work of staff. Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.

Pupils are taught what internet usage is acceptable and what is not acceptable and are given clear guidelines on using the internet. They learn about being critically aware of materials they read and

encounter and show how they then validate information before accepting its accuracy. The also learn about copyright laws.

Internet - how the school ensures safe use for pupils

Websites with potentially inappropriate content are filtered by Firewall and in the case of potentially harmful or inappropriate content, the website address and details are reported to the school's Designated Safeguarding Lead and Finance & ICT Manager for investigation. E-safety logs are also completed for each session in the ICT suite to monitor computer use.

The school also has a firewall, website filters and anti-virus software in place to provide safe internet usage for staff and pupils. These are managed by the school's outsourced IT management provider.

All pupils have their own computer log in credentials which facilitate internet usage monitoring by the school and provider.

If staff discover websites with potentially inappropriate content, details of the website are forwarded to the Finance & ICT Manager so that the website is placed on the schools 'black list'.

Internet - how unsafe or inappropriate use is managed

Any inappropriate internet use by pupils will referred the Designated Safeguarding Lead and involve the Senior Management Team. Complaints about incidents of unsafe or inappropriate internet by staff are referred to the Head Teacher verbally or by email.

Email

The school uses Office 2016 for emails. Staff can only use their default e-mail account on school systems.

How the school ensures safe email usage

Pupils are taught how to compose and send e-mails but do not have e-mail use in school unless part of lessons. Any other form of e-mail use must be agreed by the school beforehand. Personal e-mail or messaging between staff and pupils should not take place and the forwarding of chain letters is not permitted.

Staff inform the Finance and ICT Manager if they receive an email with a suspicious attachment or an offensive spam email from an external source. The school email system has a facility for blocking potentially harmful senders and messages.

Website

The Finance and ICT Manager has overall responsibility for the website. Working with Senior Management Team, website content is accurate and appropriate. The point of contact on the website is the school address, email address and telephone number. Pupil images on the website show only those pupils from whom the school has parent or carer consent. Pupils full names will not be used anywhere on the website.

YouTube

YouTube is used for educational purposes and staff must use their school log ins only . YouTube is not automatically available, with access provided by the Finance & ICT Manager.

- YouTube is used for teaching purposes only and not for commercial benefit and staff need to be vigilant to lock and secure devices with YouTube playing to prevent non-permitted access
- Pupils do not have access to YouTube on any device unless checked for suitability beforehand and always then under direct supervision of an adult
- Copies or downloads of YouTube Videos cannot be made as this is copyright infringement

Instagram, Facebook and other Social Media

Staff and pupils are not allowed to access social media platforms on school devices and staff must not list the school as their employer on their personal accounts.

Games consoles

Pupils are allowed to use games consoles as a part of their after-school club activities which are always supervised and for specific work or activities through each pupil's key work session. Only age appropriate games are allowed.

Each console must not be connected to the internet other than when updates are carried out by a member of staff. Each console is updated using ethernet cables and not WIFI.

Pupils must be monitored when using games consoles especially when the games facilitate chat rooms.

Newsgroups and forums

Access to newsgroups and forums is allowed if linked to an educational activity.

Mobile phones

Pupils have no access to mobile phones at school. Staff mobile phones and electronic photographic devices will not be used in pupil spaces during the school day. They should be kept on silent in a locker or staff transport vehicle when not in use.

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

Staff are made aware of the E-Safety policy as part of their induction to the school and all staff are given a copy of the policy to reference.

All staff must accept the terms of the 'responsible Internet Use' statement before using any internet resource in school

E-Safety and General Data Protection Regulations (GDPR) 2018

GDPR Responsibilities

The main differences between GDPR and the Data Protection Act 1998 which it replaced, is the focus on consent i.e. that parents and carers agree to schools holding data about their children and secondly, the enhanced rights that children have over their data. Personal data is defined as any information that relates to an identifiable living person. Therefore, at school, this includes pupils, parents and carers, staff and governors.

The school needs to ensure that it has proper measures in place to keep personal data safe and secure and to maintain good records of data storage. If the school suffered a data security breach and personal data was accessed from outside the school without authorisation, the school should be able to know of the breach and be able to report it to the Information Commissioner's Office within 72 hours of the breach occurring.

Data Protection Officer

Under GDPR, the school has to have a Data Protection Officer. The Finance and ICT Manager is the Data Protection Officer for the school. The main responsibilities of this role are:

- Fair and lawful processing of data
- Data accuracy and transparency
- Secure data retention
- Robust record keeping i.e. accountability

In order to ensure data security and to aid adherence to GDPR, the school has controls in place.

GDPR Article 5(1)(f) – Security Principle

The school is aware of this basic principle that data is:

"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

GDPR Article 32(1): - Security of Processing

The school is aware of this basis of secure data processing:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"

GDPR Article 35(1): - Data Protection Impact Assessments

The school is aware of data protection impact assessments:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data..."

Communication the purpose for data processing

The school has an IT Resources Usage and Data Security guidance document. The document details staff responsibilities for processing data and is read and understood by all staff.

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