ONLINE SAFETY POLICY

Author's Name	Steph Johnson
Date Written	Autumn 2017
Review Date	Autumn 2019

Date Ratified by Governing Body	Autumn 2017

Creating a Safe ICT Infrastructure in School

All users of the school's computer network have clearly defined access rights, enforced using a username/password login system. Account privileges are achieved through the file/folder permissions, and are based upon each user's particular requirements – children have greater limitations in place through a standard key stage login than individual staff members do with their personal logins, for example. This reduces the risk of accidental or malicious attempts to threaten the security of it or the data that is accessible using it.

Guests (e.g. supply teachers) are requested to login using a visitor login to prevent them viewing any potentially confidential data that might be stored on the schools' drives.

A permanently-enabled filtering system is provided, which is designed to filter out material found to be inappropriate for use in the education environment. As an additional safety measure, each individual web page is also dynamically scanned for inappropriate content as it is requested, categorised by its content and then access prevented to it if necessary.

Access to make changes to over-right the base-default setting to allow or deny access to a particular website URL can be achieved by contacting the ICT co-ordinator. All changes made to Internet filtering are logged by them to help prevent abuse of the system.

Security software is installed on all computers and tablets to prevent any malware (e.g. virus) attacks.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have ***logged off the system*** when they have completed their task and to keep their user credentials confidential to halt impersonation on the network.

Rules for Publishing Material Online (inc. Images of Pupils)

All teachers must check the photograph consent forms for parental permission for photographs prior to taking any images.

Whilst we wish the school's website to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be kept in mind, in accordance with the school's *Child Protection Policy*:

- If an image/audio/video recording of a child is used then they should not be named (including in credits).
- If a pupil is named, their image/audio/video recording should not be used (no surnames should be published).
- Files should be appropriately named in accordance with these principles and care should be taken to include only suitable ALT tags as well, (ALT Tags, alternate text when an image on a Web page cannot be displayed).
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published.
- All material is signed off by a member of the senior leadership team.

Comments submitted to posts on the website must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).

Children will likely use a variety of online tools for educational purposes during their time at the school. They will be asked to only use their first name or a suitable avatar, (Avatar, an image used to represent a person), for any work that will be publicly accessible and be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photo/videos of school events (e.g. plays) are permitted to be taken by watching parents for personal memories, they will be asked not to publish them on any public area of the Internet, including social networking sites.

Pupils' Rules for Acceptable Internet Use

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes. A copy of them is sent home to the parents of any new child and a simplified version is also displayed within school to ensure that everybody is made aware of them.

- I will ask permission from a member of staff before using the Internet.
- I will respect the facilities on offer by using them safely and appropriately.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect other pupils and myself.
- I will not download/install program files.
- I will ask permission before completing and sending forms/emails.
- I will be polite and respect others when communicating over the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details for websites with others.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

Children should be encouraged to choose strong (to include capitals, numbers and symbols) passwords to prevent unauthorised access to any of their accounts.

All children are given an account on the *Education City, Purple Mash & some to SAM Learning* virtual learning environment. This provides them with a secure area in which they: can communicate with others in their class, do homework tasks and access lesson resources. There is also a group setup on the Academy website containing useful e-safety links and another environment for communication.

Visitor's Rules for Acceptable Internet Use

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

Staff/Director's Rules for Acceptable Internet Use

Staff and Directors are contractually obliged to use the Internet safely, appropriately and professionally within school, following the same expectations and rules as given to visitors. They are aware that they are role models for others and so should promote and model the high expected standards of behaviour at all times.

Whilst checking of personal sites (e.g. emails) is permitted outside of pupil contact time, it is recognised that this should only happen for brief periods of time and is merely a privilege (not a right) and thus can be removed at any time.

E-Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential e-safety risks, as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

E-Safety education will be provided in the following ways:

E-Safety within the Curriculum

Early Years Foundation Stage and Key Stage 1
At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. Children are reminded to remain on tasks within specific apps when using tablet devices. Children will begin to use and understand simple programs, such as programming Bee Bots and accessing controlled content on Purple Mash.

Lower Key Stage 2
Children will now be given more opportunities to develop their digital literacy skills (e.g. produce pieces of work using office suite, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. Children will build upon prior programming knowledge and begin to write simple programs using programming suite.

Upper Key Stage 2
Children will now be encouraged to become more independent at researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. Children will also begin to use email, which will be catered for using an internal programme (PM). Children will design and implement code to produce a range of animations, simple games and videos.

E-Safety Training for Staff and Governors

Staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues.

E-Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive e-safety education and information (e.g. via the school website) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety behaviour – this includes delivery via the Academy website.

Guidance on the use of Social Networking and messaging systems

The school recognises that many staff will actively use *Facebook*, *Twitter* and other such social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

In accordance with school's *Child Protection Policy*, it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable not to accept as friends ex-pupils who are still minors to again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.

Data Protection

All data held on the school's network is subject to the *Data Protection Act 1998* and the school's *Child Protection Policy*. Data Protection across the Trust is currently under review in-line with the introduction of GDPR in May 2018

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school, then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data, is to be accessed off-site on a school laptop, this will be saved securely on the employee's work Microsoft One Drive account. Portable storage media must not be used unless special dispensation is agreed and an approved device is allocated. It must be recognised that this data comes under the *Data Protection Act* and is subject to the school's *Data Protection* and *Child Protection Policy*. Care must therefore be taken to ensure its integrity and security.

Staff are required to provide written consent to a responsible use contract before being allowed to use or access school IT equipment or take home school equipment (e.g. teacher laptops).

Where authorisation has been given to a specific user to use a portable storage device, the employee should utilise the agreed security software to ensure that it does not transmit any viruses onto the school's network. Any portable storage devices must be security encrypted by the IT team prior to use. Our preferred method of transferring data is the Microsoft One Drive account.

Staff are encouraged to use the shared drives on the school network as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through logon within the domain or a registered VPN by a member of school staff.

All pupil work is stored in their own personal folder on the network. Childrens' files cannot be moved or deleted whilst logged onto a machine as a pupil user.

The servers containing these networked drives are secure, with appropriate enterprise level security in place as well as back-ups and virus protection.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

Responding to Unacceptable Internet Use by Pupils

Pupils should be made aware that all e-safety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however staff are trained in how to proceed following a breach of the *Rules for Acceptable Internet Use*, in accordance with the school's *Safeguarding Policy*. This includes guidance on preservation of evidence and immediate reporting – the school's child protection officer has overall responsibility for Internet safety so any misuse should be reported to them without delay.

Depending on the severity and nature of the misuse offence, sanctions include: first warnings, temporary bans from using the ICT resources and meetings with parents/carers, all in accordance with the school's *Behaviour Policy* and in consideration of the age of the child.

All incidents should be recorded in the school's behaviour log book.

Responding to Unacceptable Internet Use by Staff and Visitors

Failure to comply with the *Rules for Responsible Internet Use* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, *Child Protection Policy* and the law. Misuse should be reported without delay.

Policy Review

This policy is reviewed regularly to respond to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.