WAKEFIELD GRAMMAR SCHOOL FOUNDATION

ICT ACCEPTABLE USE POLICY

Wakefield Grammar School Foundation ICT facilities must be used correctly and not misused or abused by users. All staff and pupils should be committed to conforming to good practice in this area. Use of the Foundation's ICT facilities implies acceptance of the conditions of use. This document sets out current policy and practice, is reviewed regularly and can be changed without notice.

Contents

Appendix

1. Introduction and Scope

1.1 Information and Communications Technology in the 21st century is seen as an essential resource to support teaching and learning as well as playing an important role in the everyday lives of both children and adults. Schools need to instruct pupils in the use of ICT in order to provide them with key skills to access life-long learning and employment. Wakefield Grammar School Foundation recognises its responsibility in educating pupils in the safe and legal use of ICT in terms of appropriate behaviour and critical thinking when using these technologies.

1.2.1 The following regulations apply to all ICT facilities and learning resources owned, leased or hired by Wakefield Grammar School Foundation, all users of such facilities and resources on the Foundation's premises and all users of such facilities and resources on the Schools' networks.

1.2.2 In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers

1.3 Staff and pupils should note the consequences of failing to comply with these regulations as set out in section 9 (Sanctions), particularly that disciplinary action may be taken by the Foundation for failure by a user to comply with them and that they may be charged for the Foundation's costs arising out of such a failure.

1.4 Staff will be expected to comply with these regulations as part of the terms and conditions of their employment. They will be given this Policy when issued with the terms and conditions.

1.5 Pupils are expected to take responsibility for their safe use of ICT facilities and all pupils are asked to sign an acceptable use agreement on enrolment at a school within the Foundation. Please note that there are separate agreements to be signed for Junior School and Senior School.

1.6 The Foundation believes that it is essential for parents or guardians to be engaged in promoting safe and responsible use of ICT facilities by their children both in and outside school. Parents or guardians are asked to read this policy and to sign an acceptable use agreement on behalf of their children along with the pupils themselves. There are separate agreements for Junior School and Senior School pupils and copies of these agreements are shown under Appendix I and II.

1.7 It should be noted that when a pupil's misuse of ICT, including cyberbullying, takes place outside school whilst using personally owned equipment or technology, and this misuse has an adverse effect on the safety and well-being of another pupil or pupils in a Foundation school, then the Foundation reserves the right to apply the Sanctions set out in section 9.

1.8 For clarification, Wakefield Grammar School Foundation includes both Queen Elizabeth Grammar School (Senior and Junior Schools) and Wakefield Girls' High School (Senior and Junior Schools).

2. Definitions

2.1 Portable Equipment – Laptop, Notebook, Chromebooks, and tablet computers and other handheld devices (such iPads, iPods, smartphones) owned, leased or hired by the Foundation.

2.2 Desktop Computers – Static desktop or Workstation computers owned, leased or hired by the Foundation.

2.3 Users – All staff and pupils of the Foundation and others outside the Foundation who have been given permission to use the Foundation's ICT facilities and learning resources.

2.4 ICT Facilities – ICT facilities located in the Schools or Foundation buildings, including networks, servers, desktop computers and portable equipment, together with the software and data stored on them, printers, other peripheral devices and any Cloud Services to which the Foundation subscribes Any ICT use carried out on equipment connected to the Foundation or Schools' networks, whether or not this involves the use of a School-based or School-owned computer.

2.5 Learning Resources – This refers to all learning resources including (but not exclusively) text, video and audio which are available to the Foundation's users.

2.6 Foundation ICT Management – The Foundation ICT Management refers to members of the Foundation Senior Leadership Team *(known as FlaG),* the Director of Studies (Operations) QEGS, the Foundation's ICT Technical Director and Senior Network Manager. The Foundation ICT Management may delegate responsibility for particular areas to members of the ICT Support Team or other appropriate School staff such as members of the Senior Leadership Teams.

3. Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. Applicable laws include, but are not limited to:

a. **EU General Data Protection Regulation (GDPR) and Data Protection Act 2018** – Together they make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

b. **Copyright, Designs and Patents Act 1998** – Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases.

c. **Computer Misuse Act 1990** – The act provides safeguards for computer material against unauthorized access or modification.

d. **Privacy and Electronic Communications (EC Directive) Regulations 2003** – These regulations prohibit the sending of unsolicited marketing emails (or SMS/text messages) to individuals. In addition the regulations control the use of "cookies".

e. **Fraud Act 2006** – This act prohibits "phishing" whereby official-looking emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.

f. **Protection of Children Act 1978** – An act to prevent the exploitation of children by making indecent photographs of them and to penalise the distribution, showing and advertisement of such indecent photographs.

g. **Criminal Justice Act of 1988 and Criminal Justice and Public Order Act of 1994** – Two acts that cover various elements of criminal law with a specific section on child pornography contained in the latter.

h. **Regulation of Investigatory Powers Act 2000** – This act allows for regulation of the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication.

i. **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** – This statutory instrument permits a degree of monitoring and record keeping to ensure communications are relevant to the business in question or to detect unauthorised use of a system.

j. Counter-Terrorism and Security Act 2015 (Section 26) – this act states that schools and childcare providers are subject to a duty, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies.

4. Use of ICT Facilities and Learning Resources

4. 1 Personal Use

4.1.1 The Foundation's ICT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by pupils in the course of their education. Any other use of the Foundation's resources puts an additional demand on those resources, which affects their performance.

4.1.2 Limited personal use of the facilities is permitted during personal time. Any such use must neither interfere with the employee's own work nor the pupil's study, nor prevent others from pursuing their legitimate work and use of the Foundation's ICT facilities. The Foundation reserves the right to withdraw this benefit either individually or collectively at any time although the Foundation will endeavour to give reasonable notice of its intention to withdraw such benefit.

4.1.3 Where the Foundation becomes aware of a specific type of personal use which affects the efficient operation of its ICT facilities, the Foundation will take appropriate steps to withdraw without notice, access to certain technology or Internet resources such as websites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with the Foundation ICT Management. The fact that a user may be able to access a particular technology or resource does not necessarily imply that the technology or resources may be accessed in accordance with these regulations.

4.1.4 Use by pupils of personal mobile technologies in school, which may or may not include camera functionality, (e.g. mobile phones, smart phones, ipods, iphones, iPads, tablets, PDAs, gaming devices, notebook computers) are subject to appropriate school rules and the conditions laid down in the BYOD Policy and Agreement Form.

4.1.5 The Foundation provides mobile technologies (e.g. mobile phones, tablets, laptops, Chromebooks) to appropriate members of staff and for use on field trips or educational visits. Only these devices should be used for Foundation business such as contacting pupils, creating images and making recordings. Members of staff should only under exceptional circumstances use their own personal devices for such business use.

4.1.6 The Foundation email system should be only used to conduct business related to Foundation activities. Personal emails should not be sent from school accounts.

4.1.7 The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Please be aware of the school's right to monitor and access web history and email use.

4.2 Commercial Use

Use of any of the Foundation's ICT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a pupil's course of study at the Foundation or a member of staff's legitimate activities) is prohibited, unless the user has explicit prior written permission from the Foundation ICT Management and an appropriate charge has been agreed between the user and the Foundation.

4.3 Movement

School ICT facilities with the exception of portable computers, tablets, smart phones should not be moved or disconnected without prior agreement of the Foundation ICT Management.

4.4 Connection – Network Access

Users must not connect any personal device into the Foundation's networks or other ICT facility without prior agreement from the Foundation ICT Management.

4.5 Damage

Users must not cause any form of damage to the Foundation's ICT facilities, software, or to any of the ICT rooms which contain equipment or software. The term "damage" includes any unauthorised installation of hardware or software, which incurs time and/or cost in restoring the facilities to their original state.

4.6 Security

4.6.1 Users must not deliberately introduce any virus, worm, Trojan Horse or other harmful or nuisance program or file into any ICT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the Foundation to prevent this.

4.6.2 Users must not attempt to penetrate the security and/or privacy of other users' files. The Foundation provides shared drives for storage of multiple users files' / folders'. Any folders or files that are intended for access only by specific individuals should be set up with the appropriate access rights in consultation with the ICT Support Team. Where such folders or files exist but no access rights have been applied then users are reminded that they must respect the privacy and not open files that are not intended for them.

4.6.3 All of the Foundation's ICT facilities have anti-virus and anti-spyware protection installed where possible. If a user suspects there may be a virus/malware on a Foundation ICT facility they should contact the ICT Support Team immediately.

4.6.4 In the interest of data security all staff should lock their computers (using Ctrl-Alt-Del or Windows-L) whenever they have to leave their computer in a logged in state.

4.6.5 Where the Foundation has provided staff with an iPad or other mobile device staff must create and apply a pin/passcode to the device which they do not share with others and is set to auto lock when not in use. This pincode should be a random set of numbers on the device. 0000, 1234 are not adequate. 6 Digit minimum should be used if possible.

4.7 Passwords

4.7.1 All users are required to keep their passwords secret and not to share them with others. Members of staff should never allow a pupil to use a computer that has been logged on to by another user.

4.7.2 Staff's passwords should meet the minimum requirement of 10 characters with a combination of mixed case letters, numbers and special characters.

4.7.3 Users will be required to reset their school password periodically.

4.7.4 Pupils attending Schools will be required to set a password with will adhere to age-appropriate password requirements.

4.7.5 Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

4.8 Phishing Spam and Mass-circulation

4.8.1 Spam is defined as unsolicited electronic messages (using email, SMS, instant messaging or other means) sent in bulk. Users may not use the Foundation's ICT facilities to send spam. Sending unsolicited electronic messages for the purposes of marketing is prohibited under the Privacy and Electronic Communications (EC Directive) Regulations 2003.

4.8.2 If a user suspects they have received phishing or spam they should not pass this on to others within the Foundation (Including ICT Support). It should be deleted or a screenshot used to capture evidence of the material.

4.9 Publishing Material Online

New technologies offer opportunities for staff and pupils to publish material online. These include blogs, forums, websites, portal content, VLEs, Wikis and podcasts. A member of the senior teaching staff will be responsible for ensuring that any content for publication is accurate, of sufficient quality and complies with the Foundation's guidelines for publication. All content must respect copyright laws. The point of contact on any published material will be the School's main contact details. Photographs with names of identifiable individual pupils will only be published in line with the Foundation's Photography and Privacy Policy.

4.10 Illegal and Offensive Material

Users must not use the Foundation's ICT facilities to access, produce, obtain, download, store, view, share or distribute material (including email, images, video, text or sound files) which is either illegal under UK law (e.g. in breach of copyright law) and/or can reasonably be judged to be offensive, likely to incite racial hatred, obscene, indecent, abusive, extremism, or raises safeguarding issues. The only exceptions would be where such material, which may be judged offensive, is essential for research or teaching, is permitted by law, and prior permission has been granted by the Foundation ICT Management.

4.11 Discrimination

Users must not use the Foundation's ICT facilities to place, disseminate or receive materials which discriminate on grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.

4.12 Defamation

Users must not use the Foundation's ICT facilities to publish any information which they know or believe to be untrue and is defamatory i.e. it could not be defended on the grounds that it is true or is fair comment on a matter of public interest

4.13 Content Creation

Content created by users using the Foundation's ICT facilities is the property of Wakefield Grammar School Foundation. When a user leaves the Foundation he or she may take a copy of anything he or she has created but this content can continue to be used by the Foundation for educational purposes.

4.14 Remote Access and Working Remotely

4.14.1 The Foundation provides staff with remote access to their folders / files stored on the school servers through the Remote Desktop login system. Users accessing the school network by Remote Access must not allow others to access the network using their login or to use their logged in computer or mobile device to access the network.

4.14.2 When working remotely if data has been removed from site via an encrypted memory stick data must not be removed from that memory stick work to be completed on the encrypted school device and returned to the network completed.

4.14.3 Memory Sticks are not storage mediums, they are for short term transportation of data. Once the offsite work is completed the data stored should be returned to the school network.

4.14.4 Staff are encouraged to use school devices for school work. All laptops must be encrypted before removal from site and use.

4.14.5 The Foundation provides access to Email and other services (Google, OneDrive, SOCS) to users through a web interface. Care should be taken not to download any content containing personal information onto a non-school device.

4.15 Bring Your Own Device (BYOD)

4.15.1 The Foundation has introduced a BYOD scheme for staff and senior school pupils, which is governed by the separate Bring Your Own Device policy and user agreement. This scheme allows staff and senior school pupils to access the respective school wireless network using their own technology (laptop, smartphone, tablet). Once on the wireless network, all users will have filtered internet access just as they would on a school owned device.

4.15.2 Any staff device which is used in a BYOD capacity and used to connect and store email and other data (Mobile Phone / iPad / Chromebook / Laptop) must be encrypted and secured by a difficult to guess pin / passcode and kept up to date with the latest security patches available.

4.16 Foundation Device Policy

The Foundation has allocated school owned devices (iPads, Chromebooks, Laptops etc) to some staff and pupils for teaching / learning and administrative reasons, which are covered under a separate Foundation Device Agreement which should be read in conjunction with this and other policies mentioned.

5. Monitoring of ICT Facilities

In order to protect the security and working of the Foundation's ICT facilities and users, it may be necessary to monitor collective or individual usage of its ICT facilities. This is particularly likely where there are indicators of abuse of systems, or that individuals may be using systems in excess of their authority. Files, messages, emails and user account information may be intercepted, monitored, recorded, copied, audited and inspected.

5.1 Confidentiality

5.1.1 Absolute confidentiality cannot be guaranteed. Any emails or files, stored and/or sent or received may be accessed by colleagues other than the individual(s) to whom it was intended whether by accident (e.g. a computer left logged on) or design (e.g. an email may need to be opened to diagnose connectivity problems, or ensure the smooth running of the school in user absence). Emails and files cannot therefore be regarded as totally private or confidential.

5.1.2 The ICT Support Team across the Foundation has total administrative access to all the Foundation's ICT facilities and has the right to monitor and access all ICT resources, including any saved files. Any misuse of ICT facilities found by the ICT Support Team will be reported to the Foundation ICT Management.

5.2 Internet Access

5.2.1 Internet access is provided for educational, administrative, research and personal development use. Pupils using the Internet will be supervised as appropriate to their age range. Teaching staff will preview any recommended websites before instructing pupils to access them. If Internet research is included in a homework assignment, specific sites will be suggested that have been previously checked by teaching staff. Parents are advised to supervise any further research. If users discover or inadvertently access an inappropriate website, the screen must be closed immediately and the incident reported to a member of the teaching staff (for pupils) or the ICT Support Team (for staff).

5.2.2 It should be noted that users of the Internet do not have a right to confidentiality or privacy when using or accessing the Foundation's ICT facilities. The Foundation ICT Management monitors and reviews network logs maintained in order to ensure compliance with Foundation policies and UK law. The Foundation uses software to track usage. The software records details of every website visited, along with the relevant user name and date/time, and produces reports for monitoring purposes. Misuse or visits to sites of an improper nature will automatically be reported to the Foundation ICT Management.

5.2.3 Internet filtering is in use throughout the Foundation to protect users from viewing objectionable / inappropriate material and guide users to appropriate websites. This filtering is tailored to be age appropriate but it should be noted that no filtering is infallible so care should still be taken.

5.3 Social Networking Sites (including Facebook and Twitter)

5.3.1 Pupils are not permitted to access Facebook and other Social Networking websites whilst using Foundation ICT facilities unless legitimate educational reasons are presented.

5.3.2 Pupils are advised to be cautious about the information given by others on these sites and likewise about information they give. They should avoid giving personal details that would enable them to be identified. Pupils are also taught to avoid placing images of themselves and others on such sites and furthermore placing of inappropriate images will lead to disciplinary action (see Section 9) and potentially legal action. Pupils are advised to set and maintain maximum privacy levels and deny access to unknown individuals.

5.3.3 Members of staff must not be in contact with current Foundation pupils via social networking sites. Furthermore, pupils must not make friendship requests to or accept friendship requests from members of staff and equally, members of staff must not make or accept friendship requests from pupils. If a member of staff receives a friendship request from a pupil then the request must be immediately rejected and the matter reported to the Deputy Head or Head as appropriate who in turn will speak to the pupil.

5.3.4 Please refer to the Foundation Social Media policy.

5.4 Email

5.4.1 Email is an essential means of communication across the Foundation for both members of staff and pupils. All users are expected to adhere to generally accepted etiquette when using email with regard to use of appropriate language and avoiding content that could be deemed offensive (see Section 4.9). When either staff or pupils are sending emails to colleagues or pupils, they should consider the following:

- think before pressing ‘send’
- never send an email in haste or in anger but take time to reflect
- use polite terms of address
- do not say anything in writing that you would not feel comfortable saying face to face
- email is not the ideal forum to raise complaints – talking things through is always the best option
- be careful to check the circulation list and the thread that may be forwarded on – some things may be confidential or inappropriate for others to see.

5.4.2 Under no circumstances should members of staff contact pupils, parents or conduct any business using personal email addresses without express permission from the Foundation ICT Management.

5.4.3 The Foundation reserves the right to retrieve the contents of email messages for the following purposes:

a. to monitor whether the use of the email system is legitimate and in accordance with this policy
b. to find lost messages or to retrieve messages lost due to computer failure
c. to assist in the investigation of misuse
d. to comply with any legal obligation
e. to enable continuity of school business in the event of the absence of a user from school

5.4.4 Monitoring will only be carried out to the extent permitted or required by law. The Foundation will not routinely manually inspect email messages. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the Foundation has reason to believe that the systems may be being used in breach of this policy.

5.4.5 The Foundation's policy towards spam is that it should be filtered upon receipt and quarantined. All effort is made to filter out spam before reaching users' inboxes, however, it should be kept in mind that spam filtering is an ongoing endeavour and is not fool proof. The occasional message may reach a user and should be deleted in the normal way. Measures are taken to ensure legitimate messages are not treated as spam but it is possible that occasional messages may falsely be identified as spam. In such cases the ICT Support Team can release quarantined emails.

5.5 Files

5.5.1 The Foundation reserves the right to retrieve the contents of files for the following purposes:

a. to monitor whether the use of the storage medium is legitimate and in accordance with this policy
b. to find any deleted files or to retrieve files lost due to ICT facility failure
c. to assist in the investigation of misuse
d. to comply with any legal obligation
e. to enable continuity of school business in the event of the absence of a user from school

5.5.2 Monitoring will only be carried out to the extent permitted or required by law. The Foundation will not routinely monitor files. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the Foundation has reason to believe that the systems may be being used in breach of this policy.

5.6 Storage – Personal Folders and Departmental Shared Drives

5.6.1 Each user receives a personal folder, which is private to them and accessible via the network. A maximum quota is imposed to prevent the server from being filled by a few users.

5.6.2 Please note that the ICT Support Team has administrative privileges and access to personal folders and all files stored on the Foundation's ICT facilities. Users should not store personal photos, images or music files in personal folders; they are designed for storing work files only.

5.7 Software

5.7.1 Users of the Foundation's network are not authorised and are unable to load any software onto the ICT facilities. Only software licensed to the Foundation or one of the Foundation Schools may be installed on the Foundation's ICT facilities. It is forbidden under any circumstances to run peer to peer (P2P) software on any of the Foundation's ICT facilities.

5.7.2 Software downloaded from the Internet may only be loaded onto the Foundation's ICT facilities with prior permission from the Foundation ICT Management. Any software obtained and/or installed illegally will be reported to the Foundation ICT Management.

5.8 Removable Media and Online Storage

5.8.1 Removable media refers to computer storage devices which are not fixed inside a computer and include tapes, floppy disks, removable or external hard drives, DVDs, CDs and solid state memory devices such as memory cards, pen drives or memory sticks. Online storage refers to internet based file storage solutions (e.g. Microsoft One Drive, Google Drive, Drop Box)

5.8.2 Users are responsible for ensuring that files transferred to Foundation facilities are free from viruses or other harmful programs.

5.8.3 It is the responsibility of users to ensure that any information accessed from their own computer, removable media or online storage is kept secure and that no personal, sensitive or confidential or classified information is disclosed to any unauthorised person.

5.8.4 No personal, sensitive or confidential or classified information relating to other individuals should normally be taken off the Foundation premises. However, where staff need to take such information off the Foundation premises for trips / further work / development then the ICT Support Team will provide staff, on request, with an encrypted USB flash drive or other encrypted device.

5.9 Online Curriculum Resources and Administration Services

5.9.1 The Foundation subscribes to many online services which help the Foundation's schools teaching and learning objectives, trips and day to day administration. To access these services appropriate data for that service about staff, pupils and contacts may be shared with particular services.

5.9.2 Before subscribing to any new service staff should consult the Foundation ICT Management Team to ensure any service complies with all relevant legislation and information kept to their compliance.

5.9.3 Examples of the above services include but are not limited to :- Google G-Suite, Microsoft Online Services, Parent Pay, Firefly, Mathletics, SOCS, Hegarty Maths, Active Learn, Eclipse, Oliver.

6. Maintenance and Repairs

6.1 Maintenance is to be controlled by the ICT Support Team which may be in conjunction with approved external suppliers. From to time ICT facilities especially portable computers will be recalled by the ICT Support Team for maintenance purposes. It will not be possible to support the Foundation's ICT facilities if equipment is not correctly maintained. Any faulty or defective ICT facility should be reported to the ICT Support Team as soon as the problem is identified.

6.2 The ICT Support Team will attempt to recover any data stored on faulty ICT facilities but it cannot be guaranteed.

7. Copyright and License Agreements

7.1 Users must adhere to the terms and conditions of all license agreements relating to ICT facilities and learning resources which they use including software, services documentation and other goods.

7.2 Users must not copy or modify any copyright material nor incorporate any part of any 3rd party material into their own work unless such acts are either permitted under the Copyright, Design and Patents Act 1988, by a license agreement or with the permission of the copyright holder.

8. Behaviour

8.1 Users must respect the rights of others and should conduct themselves accordingly when using ICT facilities to create a beneficial environment for all.

8.2 Users must not interfere with or disrupt the availability and use of the ICT facilities by others.

8.3 Users must take every precaution to avoid damage to equipment and learning resources caused by the presence of food or drink in its vicinity.

8.4 Users must respect the access rights of others and the content of files contained within folders on any drives. The content of any file should not be changed without the knowledge and / or permission of its author.

9. Sanctions and Breaches of this policy.

9.1 Withdrawal of facilities

If a user is in breach of any of these regulations then the Foundation ICT Management may withdraw or restrict the user's use of ICT facilities and learning resources. This will be in consultation with the Head or Deputy Head of the School and/or Bursar if the user is a member of staff or with the Form Tutor, Head of Department and parents if the user is a pupil.

9.2 Removal of Material

The Foundation reserves the right to remove material from its ICT facilities without notice where such material is in breach of these regulations.

9.3 Disciplinary Action

Any breach of the regulations which has been identified by the Foundation ICT Management may be dealt with by the Head (or Deputy Head) or the Bursar under the Foundation's or Schools' respective Behaviour and Discipline policies for pupils and the Foundation's Disciplinary Procedure for members of staff. In some cases this may result in suspension, expulsion or dismissal. Parents will also be informed if disciplinary action is to be taken against pupils.

9.4 Cost Recovery

Where damage to Foundation ICT facilities has resulted from failure by a user to comply with this policy, the user may be charged for the Foundation's costs arising out of such a failure.

9.5 Breaches of Law

Should the situation arise, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

9.6 Breaches of this policy

If you become aware of a breach of this policy please inform the Foundation ICT Management as soon as possible.

9.7 Concerns

If you are concerned that a member of the school community is being harassed or harmed online you should report it to the Designated Safeguarding Officer in your school. Reports will be treated in confidence. See Safeguarding Policy.

10. Retention of Digital Data

Data in the Foundation systems is subject to a separate Data Retention Policy.

11. Breach Reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Please refer to the Foundation Breach Reporting Policy.

12. Disclaimer

The Foundation accepts no responsibility and expressly excludes liability to the fullest extent permitted by law for the malfunctioning of any ICT facility or part thereof whether hardware, software or other facility or for the loss of any data or software or the failure of any security or privacy mechanism.

Review History

Policy written	February 2011	L Perry/J Lister/M Lassey
Policy updated	August 2013	L Perry
Policy updated (social media)	October 2014	R Clarkson
Policy updated (email)	March 2015	L Perry
Policy updated (prevent duty)	October 2015	R Clarkson
Policy updated (general)	March 2016	R Clarkson
Policy updated (general)	October 2017	L Perry/J Lister
Policy updated (general)	May 2018	J Lister
Policy updated (general)	June 2018	J Lister
Policy updated (general)	September 2018	J Lister

Appendix I: Prevent Duty

The Foundation's schools are committed to providing a safe and secure environment for pupils, where children feel safe and are kept safe. Safeguarding our pupils in the course of accessing content online is covered, as well as in this appendix, in the following policies:

- Foundation Safeguarding Policy (s1, page2; s4.4.3, page12)
- QEGS JS ICT Policy
- Junior School Acceptable Use Pupil Agreement Form
- Senior School Acceptable Use Pupil Agreement Form
- Bring Your Own Device (BYOD) Policy
- Bring Your Own Device (BYOD) Pupil Agreement Form

The purpose of this Acceptable Use Policy update is to address the context of safeguarding from an ICT perspective in reference to Prevent duty. The sections below refer to the technical measures that the Foundation employs to protect children, and the behavioural rules and expectations when pupils go online to access content.

1. Technical Security

The Foundation will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc… from accidental or malicious attempts which might threaten the security of the school systems and data. These are:

1.1 Internet filtering and Firewall

The Foundation takes a multi-layer approach to Internet Filtering and Firewall provision. There is a perimeter hardware firewall with some basic filtering in place and a proxy for more targeted at content filtering.

The firewall is used to monitor and control the incoming and outgoing network traffic in order to protect its users. It employs the latest unified threat management processes and, together with its secure web gateway, provides a high level of perimeter and internet filtering protection to the network.

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

The software firewall uses the Home Office terrorism blocklist to block terrorist content as per Government guidelines. Its in-house categorisation team have also extended this category beyond the Home Office blocklist to offer further protection against terrorist and extremist content.

Its reporting suite allows us to monitor and report all user access in real time when requested.

1.2 Network content analysis software

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment using a specific software application.

The software is used across the Foundation schools as a classroom monitoring, network management and user management application. Whilst it will not indicate that an attempt to access a particular web site or that a potentially concerning communication has been sent or received, it does log the actions of all users logged onto WGSF network. It will only do this, however, on a computer or laptop on which the software has been installed. Additionally, the software allows remote screen viewing of computers and laptops connected to the network allowing ICT support to screen capture, communicate and take control of a user's device.

"The software has been specifically designed with intelligent safety features that provide e-safety for schools. Schools are empowered to safeguard students from potential online risk using keyword detection, blocks and filters fused with acceptable use boundaries. Real-time monitoring and alerts exposes violations, which serves to prevent incidents materializing in the first instance."

The ICT support team use this software as a reactive tool in that whenever any incidents are reported its logs are scrutinised to obtain evidence, which is date and time stamped, relating to the incident.

1.3 Anti-virus, spam and malware

The Foundation takes a multi-layer approach to Antivirus, Spam and Malware. The firewall edge device does a first level of Antispam, Antivirus and Malware at the network perimeter before the anti-virus software takes over at the desktop and server level.

The anti-virus software is used for web and e-mail protection against viruses, malware and spam. Their labs provide continual intelligence up-dates on the latest malware hosting, phishing and distribution sites as well as anonymising proxies and other sites. It then provides updates in real time via their Live Protection network.

The software employs the latest antivirus and phishing detection technology that constantly
updates in real-time to detect the latest threats. It also blocks unwanted content using MIME type and extension filters.

e-Mails and any attachments are analysed on receipt at the server before being passed onto the user checking for abusive language as well as traditional antivirus, spam etc.

2. Behaviour and Expectations

In addition to the expectations governing staff, pupils and visitors given earlier in this document, the following additional rules must be followed whilst on the Foundation premises and accessing content electronically, whether it is on a Foundation device or their own. This includes SMS messages, use of social media and internet content and applies to anyone using the Foundation's internet, WiFI or e-mail systems.

Staff, pupils and visitors are not:

- To access web sites that promote extremism, radicalisation or terrorism.
- To submit or publish personal information about themselves or others (including 'selfies') unless part of an approved educational activity. This includes using apps, micro-blogging sites such as Twitter, blogging, social networking, personal web pages, VLE, e-mail systems, SMS, online forums & chat or any other web based public information and collaboration systems and any app service.
- To access, store or share 'unsuitable' or illegal material on any Foundation IT system or your own tablet or personal telephony device. Unsuitable material includes (but is not restricted to) gambling, pornography, promotion of bullying, sexual exploitation, extreme violence or sites inciting hatred of a particular group. Where internet access is gained outside of the school network e.g. via Mobile 3G/4G, the same rules apply in terms of not accessing 'unsuitable' material.
- To use anonymising proxies to circumvent the Foundation's security systems. This is strictly forbidden.

References

- https://www.gov.uk/government/publications/prevent-duty-guidance
- DfE Guidance "Keeping Children Safe in Education, 2018"
- DCSF Resources "Learning Together to be Safe", "Prevent: Resources Guide", "Tackling Extremism in the UK"
- UK Safer Internet Centre web site: http://www.saferinternet.org.uk/