Harton Academy

e-Safety in School

Reviewed Sept 2023
Next To be reviewed in Sept 2024

1 Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

As a school we must demonstrate that we have provided the necessary safeguards and done everything that could reasonably be expected of us to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2 Scope of the Policy

2.1 This policy applies to all members of the academy community (including staff, students, trainees, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

2.2 The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

2.3 The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3 Our Policy

3.1 Students and acceptable use

Whilst regulation and technical solutions are very important, the use of technology must be balanced by educating students about its benefits and also to take a responsible approach to its use. Education in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need help, support and guidance to recognise and avoid e-safety risks and build their resilience.

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

- e-safety should be provided as part of the ICT curriculum / PHSE / other lessons and should be regularly revisited – covering both the use of ICT and technologies in and outside of school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be posted in all ICT suites and displayed on log-on screens.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

3.2 Parents and Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The academy will therefore seek to provide information, guidance and awareness to parents and carers through various means, as appropriate.

3.3 Curriculum

E-safety should be a focus in all areas of the curriculum and all staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to a range of sites, checked as suitable for their use, and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. In ICT suites full use should be made of the room control software (Impero) which allows staff to monitor, and if necessary control access to various sites and the internet as a whole.
- It is accepted that, from time to time and for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. When necessary, staff can request to temporarily remove those sites from the filtered list for the period of study. Requests should be made to the E-Safety Officer.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. They should also be taught good search skills and techniques to refine their searches effectively.
- Students should be taught to acknowledge the sources of information used and to respect copyright when using material accessed on the internet.

3.4 Acceptable Use

All members of the academy community shall be expected to adhere to the acceptable usage rules. These are provided as appendix 1. Access to equipment and systems is dependent on an individual's acceptance.

The Acceptable Use agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

The agreement provided in Appendix 1 will be shared with pupils in classrooms and in tutor bases. It is expected that every time a pupil uses computer equipment or software, they are agreeing to this policy.

4 Roles and Responsibilities

4.1 Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The review of procedures and effectiveness will be carried out by the Governing Body

or appropriate sub-committee and will receive regular information about e-safety incidents and monitoring reports :

- regular meetings with the E-Safety Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

4.2 Senior Leaders

The Headteacher and Senior Leaders are responsible for :

- ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- ensuring that training outlined in this policy is undertaken by relevant staff
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

4.3 E-Safety Officer

The E-Safety Officer is responsible for

- leading the e-safety committee.
- taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- ensuring that all staff are aware of the school's procedures that need to be followed in the event of an e-safety incident taking place.
- providing regular training/updates and advice for staff.
- liaising with the Local Authority.
- liaising with school ICT technical staff.
- maintaining a log of incidents by the ICT Support Manager to inform future e-safety developments
- meeting regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- providing reports to Senior Leadership Team as required.

4.4 ICT Support Manager

The ICT Support Manager must ensure they are fully aware of the NGfL Security Policy and Acceptable Usage Policy and the South Tyneside guidance on e-safety and they keep up to date with current practice.

4.4.1 The School's ICT Support Manager / ICT Technicians are responsible for ensuring:

- the security of the school's ICT infrastructure so it is not open to misuse or malicious attack.
- the school meets the e-safety technical requirements of the provider of connectivity services

- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- that the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person, but is jointly agreed by the senior school technician (ICT Support manager) and the E-Safety Officer.
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network, remote access and email systems are regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Officer
- that monitoring software / systems are implemented and updated as agreed in school policies.

4.4.2 The academy's VLE Manager / Website manager is responsible for ensuring:

- that the use of the Virtual Learning Environment (VLE), is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Officer.

4.4.3 Teaching and Support Staff are responsible for ensuring that they:

- have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP), and have read the student AUP.
- report any suspected misuse or problem to the E-Safety Officer and other appropriate member of the senior leadership team.
- ensure digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- embed e-safety issues in all aspects of the curriculum and other school activities.
- ensure students understand and follow the school e-safety and acceptable use policy.
- ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- monitor ICT activity in lessons, extra-curricular and extended school activities.
- are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.6 Designated Safeguarding Lead

The Designated Safeguarding Lead and deputies should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

4.7 E-Safety Committee

Members of the E-safety committee (or other relevant group) will assist the E-Safety Officer with the production, review and monitoring of the school

- e-safety policy / documents
- filtering policy, data management policy and password policies.

The committee should include representation from students and parents / carers and various types of staff and governors.

5 Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that systems used are as safe and secure as is reasonably possible.

- Academy ICT systems will be managed in ways that ensure that the school meets the E-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems. This will now also include penetration testing by using some software tools that we are currently researching (2023) and/or a third party penetration testing and consultancy test by Blackberry or a similar consultancy firm.
- Servers, wireless systems and cabling must be securely located and physical access restricted, e.g. only school technical staff, via ID card and key access to main server room (including caretakers in emergency).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Support department and will be reviewed, at least annually, by the E-Safety Committee. Requests to the ICT support team to change such access rights **must be supported by an email from senior staff or the Headteacher which must be retained in ICT records as evidence.**
- All users will be provided with a username and password by the school's technical staff, who will keep an up to date record of users and their usernames. Users will be required to change their password every three months or every term (currently temporarily disabled). A school password policy is provided in the appendix to this document)
- The "administrator" passwords for the school ICT system, as used by the school's ICT technical staff must now also be available to the Headteacher or other nominated senior leader and Director of ICT/ E-Safety officer, and kept in a secure place (e.g. school safe in Finance) from Sept 2023.
- The academy should never allow one user to have sole administrator access. Currently we have a network manager and technician who both share access to the main administrator account, along with the School's Director of ICT and similar access to most passwords is available to our third line support company, with restrictions on when they can gain remote access.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The academy subscribes to 'Smoothwall' who provide us with a cloud-based managed filtering service via our own user portal, accessed through our Service Provider Durham County Council ICT Support Service (formerly Durham NET) to provide full internal control of our filtering needs – this is updated regularly online and has been in use since 2017. The system is linked to our Active Directory system so that we can provide full granularity of access, down to individual users and their filtering requirements. This provides filtering by domains and by specific URLs in the form of standard blacklists and/or whitelists but also allows for additions to that filtering, upon our own research and testing, by school ICT staff, if requested by colleagues.
- In the event of the School's Senior technician (or other member of the technical staff) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by agreement with the Headteacher (or E-Safety Officer).
- Any filtering issues should be reported immediately to Smoothwall, via the ICT support team to get them resolved.
- Filtering will also be tested regularly, termly at first, inserted in the ICT support calendar (using aids and tests such as 'testfiltering.com') with the results passed to the ESafety officer and through him to Senior management and Governors.
- Requests from staff for sites to be removed from the filtered list should be sent by email and will be considered by the E-Safety Officer (or nominated member of senior leadership team) and Senior school technician on site (n.b. an additional person, such as the senior school technician should be nominated to agree such decisions, to ensure protection for the E-Safety Officer or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- The academy has provided enhanced E-Safety monitoring through the use of the Impero network monitoring tool and classroom management system/ keystroke monitoring system, relying on both monitoring of alerts by ICT suite teachers, through their dashboard (showing individual thumbnail display of student screens) and monitoring by ICT support and management staff who check regular reports of alerts generated within the whole estate. Such reports need to be examined daily so, due to the high level of false positives caused by the 'wildcard' type searches recommended by agencies specialising in the Prevent initiative, Violence, Grooming, Pornography, Racism, Gambling, and other forms of extremism and prejudice we are in the process of researching and adopting a managed service for such monitoring, probably 'Smoothwall Monitor.' This uses a combination of AI and human pre-qualification of alerts and elimination of false positives and informs the school's designated Safeguarding Leads by email and phone of any genuine causes for concern found in network activity (of any sort) identifying the user, machine, date and time of the incident – **this must then be followed up with urgency**. Such software may well be used to link outcomes into CPOMS once the DSL has checked the relevance of any alerts provided.
- Academy ICT technical staff regularly monitor and record the activity of users on the school ICT systems remotely, and users are made aware of this in the Acceptable Use Policy.
- Remote management tools such as the Impero are used by ICT and general teaching staff to control workstations in ICT suites and banks of laptops, and to view users' activity. This is intended to be used to supervise class use of ICT equipment but may occasionally include others who happen to use this equipment.
- An appropriate but simple system is in place for users to report any actual / potential e-safety incident / concern to the E-Safety Officer (or other relevant member of senior management). This is done via an email link on the school VLE system and we are setting up an anonymous internal mail feature to the E-Safety officer
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which

might threaten the security of the school systems and data. These include Microsoft Endpoint Antivirus software, the latest up to date software and firmware versions for our Watchguard firewalls and all servers must be fully updated to the latest security patches.

- Visitors and Guests - An agreed policy is in place for the provision of temporary access for "guests" (e.g. trainee teachers and visitors) onto the school system. This requires that such users can be identified while using the equipment and its software. Visitors may be given a specific recorded guest account and temporary password to allow them access to the internet, on a loan laptop or tablet, upon request (fully filtered wireless access to the internet alone, not the school network, like that used by students).
- If authorised visitors (such as Local Authority staff, support workers, Visual Impaired Service etc.) need to bring their own devices on site to use specific software while working with students or staff, that is permitted as long as they do not need to connect to the school network or internet, this approval should be checked with ICT Support staff in advance. We do not allow visitors to attach their own devices to the school network as this poses a security threat and they may introduce viruses, malware or inappropriate materials onto our network.
- Certain visitors or guests may be given a temporary password to the school network in certain circumstances, e.g. training of staff etc., but with very limited access rights to their own document area only. Student teachers will be trained in the use of the network, given a 'trainee' account and password for the network and for SIMS to allow them to register classes while teaching. This will only be allowed once they are fully DBS checked. Such visitor access restrictions will remain in place until our external device management system is set up, so that we can fully filter and monitor their activity on the internet or their devices while on site.
- We are investigating a full management system to allow third party devices to be joined to our network via a piece of client software that would alter the user experience while on the school site, then possibly remove itself or lie dormant when the user leaves the site. This would allow us to add student owned laptop and tablet devices to the network broadening the volume of resources available to students during lessons and private study.
- We are changing the use of IPads and other tablet devices to ensure that all require the user (Student or staff) to log in with their password protected account – this is to ensure that no devices can be used without the user being identifiable through monitoring and for filtering purposes. We are seeking to lock our Kindle Fire devices so that they can only be used for reading prescribed materials (e.g. downloaded online books) and not access the internet or provide unmonitored text access.
- An agreed policy is in place (to be described) regarding the downloading of executable files by users. It is currently blocked by the Network group policies due to the risk of malware infection brought in via executable files.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy Template in the appendix for further detail)
- An agreed policy is in place that blocks staff from installing programmes on school workstations or portable devices, the exception to this being use of a personally allocated staff laptop on which they may install some acceptable software and utilities that will aid their use of the device for lesson and resource preparation.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices such that all memory sticks and external drives must be tested for viruses and malware by the ICT support team before use. (see School Personal Data Policy Template in the appendix for further detail). This means that colleagues bringing visitors to site to take part in assemblies or training or staff or students, will need to ensure that they are aware that all their materials must be checked as soon as they arrive.

- The academy infrastructure and individual workstations are protected by up to date anti-virus software, currently Microsoft Endpoint security, which must be regularly updated.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy in the appendix for further detail)

7 Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves, or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The academy will inform and educate users about these risks to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. If, by force of circumstances, some images have been taken on personal equipment, such as Smart phones, they should be moved onto school equipment (e.g. network storage area) as soon as possible upon return to school and any copies deleted from personal equipment.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published in full with the permission of the student and parents or carers.

The School has adopted a separate policy for the Use of Images of Students.

8 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 & 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights

- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data and that such data is not accidentally shown over a classroom projector (N.B. use of the 'Freeze' button when editing student data while using a whiteboard and projector).
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

9 Training and Education in E-Safety

9.1 Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff may identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Officer (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by LA / CEOP (Child Exploitation & Online Protection Agency) and others.
- Staff will be briefed on this policy and any updates or related areas as required.
- The E-Safety Coordinator will provide advice / guidance / training to individuals/departments as required.

9.2 Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT / E-safety / health and safety / child protection.

Appendix One

ICT Acceptable Use Policy for Pupils and Students

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

The below agreement will be shared with pupils in classrooms and in tutor bases. It is expected that every time a pupil uses computer equipment or software, they are agreeing to this policy.

User Agreement (Pupils and Students)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

I understand that the school will monitor my use of the ICT systems, devices and other digital communications :

- I will keep my username and password safe and secure. I will not share it, nor will I try to use any other person's username and password.
- I will ensure I undertake safe practice whilst online to ensure my own and others safety.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems and devices are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems and devices for anything other than educational purposes unless permission has been given.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal devices in school if I have permission or during social time. I understand that if I do use my own devices in school, I will follow the rules set out in this agreement in the same way as if I was using school equipment.
- I will not open links or attachments unless I know and trust the organisation it came from.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites on school equipment or during learning time.
- I will not walk around the school using a mobile device, oblivious to all around me

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action in line with school procedures.

I agree to use the school provided email address solely for educational purposes. This means that I will not:

- Send offensive or upsetting messages or content to any user
- Sign up to newsletters or join online communities unless specifically recommended by one of my Teachers
- Use any account other than my own.

I understand that the school monitors the emails I send for safety and security reasons.

I have read, understood and agree to the rules included in the ICT Acceptable Use Policy.

ICT Acceptable Use Policy for Staff, Governors, Volunteers and Trainees

General Conduct and Use

All academy staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use providing that this is not :

- Taking place at the expense of contracted hours
- Interfering with the individual's work
- Relating to a personal business interest
- Involving the use of news groups, chat lines or similar social networks
- At a cost to the school
- Detrimental to the education or welfare of students at the school

Any damage to equipment should be reported to ICT. The same applies to any apparent malfunction of equipment.

Use of the Network

- When logging on to the network, staff must always use their own user identification and password.
- Any member of staff who identifies a security problem on the network must notify ICT immediately.
- Staff must never divulge their passwords or write them down unless required to do so by ICT for support purposes. Any member of staff who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay and report this potential security breach to ICT.
- Staff must not use the network to gain unauthorised access to any other computer network.
- Staff must not attempt to spread computer viruses.
- Staff must understand that the information they hold on the network is not private.
- Staff must not store personal documents/pictures/music on their school documents area.
- Before leaving a computer, staff must always log off the network or lock their terminal and check that this procedure is completed.

Data Protection

Data protection is the responsibility of all members of staff.

- Staff must not disclose to a third party the personal details of another member of staff, a pupil or a pupil's family. When sending emails, staff should ensure the anonymity of addressees by making use of the BCC (blind carbon copy) functionality when addressing emails.
- Staff must ensure that they do not retain copies of the personal details of another member of staff, a pupil or a pupil's family on their devices. Further to this, paper copies of lists and/or other pupil data should not be taken home.
- Staff must ensure that devices connected to school accounts are kept secure whilst in and out of school and report any loss to ICT immediately.
- Staff must not store school material on cloud folders, USB sticks or external hard drives.
- Do not disclose sensitive data to third parties without prior authorisation.
- Staff should also refer to the School Data Protection Policy.

Internet and E-mail

Email Rules

- Staff must not send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
- Staff must not make inappropriate use of the email system and address book, such as sending bulk emails, chain emails or for personal marketing purposes.
- Staff must not use their email account to send or exchange material of an undesirable or illegal nature.
- School email accounts should only be used for purposes relating to school matters.

Internet Rules

Whilst the academy internet facilities exist principally for enhancing the educational purposes of the school, staff may make personal use of the internet in their own time provided this doesn't detrimentally affect the school's primary function.

Staff should also be aware that all internet usage is logged.

- Staff must not breach another person's copyright in any material.
- Staff must not attempt to access inappropriate websites using the school network and should be aware that all websites accessed are logged.
- Staff must not upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
- Staff must not engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden.

Software

- All academy installed software is subject to change and may be updated or removed at the academy's discretion when deemed necessary.
- Staff should not attempt to alter or remove any software installed on school computers without consultation with ICT.

Laptops & Mobile Devices

Staff are provided with either a laptop or mobile device for the better performance of their teaching and/or administrative duties. Laptops will be fully supported and maintained by ICT and mobile devices will be supported in the connection to school services. By accepting the provision of a laptop/mobile device, staff agree to the above policy and in addition the following rules:

Connection to the network

- In order to help keep the network secure, safe and virus free, connection to the School network of any unauthorised device is strictly forbidden. The only devices that can connect to the School network are those which have been authorised by ICT.
- School laptops should be connected to the school network at least once a week to ensure that any necessary windows/software/antivirus updates can take place.

- Staff must ensure that non-school devices connected to the network are kept secure and have up-to-date antivirus software. Any devices with known vulnerabilities on will be removed from the network.
- Under no circumstances should any school equipment be detached from the network to make way for a laptop/mobile device.

Damage or loss

- The academy cannot accept responsibility for any damage caused to laptops or their contents (files, folders etc.) by inappropriate use.
- Any damage to laptops or mobile devices, whether accidental or otherwise, should be reported to ICT as soon as possible.
- A charge may be incurred if a school owned laptop/device is damaged by improper use. A charge may also be incurred to cover insurance excess if the laptop/device is lost or stolen due to insufficient security.
- Whilst in transit, laptops/devices must be stored out of site, preferably in the boot of the car. If the car is left unattended then the laptop/device MUST be stored in the boot, out of site. Failure to do so will negate the school insurance cover and the member of staff may be liable for the cost of a replacement.
- At home, laptops/devices must also be stored out of site, preferably in a locked draw or cupboard, when not in use.

Licensing and copyright

- It is the responsibility of the owner to ensure that they have a licence for any additionally installed software over and above that which is already provided with the laptop/device.
- Staff are responsible for ensuring that the copyright of media files (music, images and video) is not breached by illegal copying of such files.
- Staff are responsible for the material that exists on or is accessed via their laptop/device.