HOLYROOD
ACADEMY

POLICY

E Safety

Guidance Policy for ICT Acceptable Use

March 2020

Next review date: September 2020

Contents

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including, web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the online technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting or blogging
- Music Downloading & streaming
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these online technologies.
At Holyrood Academy we understand the responsibility to educate our pupils about eSafety and online issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our schools to use technology to benefit learners.
Everybody in the Academy has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
This policy is inclusive of both fixed and mobile internet technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises (including but not limited to PCs, laptops, tablets, mobile phones, webcams, whiteboards, smart TV's, voting systems, digital video equipment, etc.

Monitoring

ICT Support staff authorised by the Headteacher or their designated deputy may inspect any ICT equipment owned or leased by the Trust at any time without prior notice. ICT authorised staff may also monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/ intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Trust or School business related information; to confirm or investigate compliance with Trust and School policies, as part of a disciplinary investigation; standards and procedures; to ensure the effective operation of Trust and School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or any data stored in the Trust system, or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using Trust ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All activity is logged by the Academy. These logs are monitored by the IT Manager reporting to the Designated Safeguarding Lead. Certain keywords are flagged which may result in a screen shot being saved

Policy Breaches

Any policy breach may be grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Data Breach Reporting

Any loss of data, security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Trust IT manager or Data Protection Officer. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Trust IT Manager.

ESafety

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Trust, the CEO and the directors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Each school within the Trust will have a member of its Senior Leadership Team designated as the eSafety co-ordinator for that school. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection), Childnet & UK Safer Internet Centre.

Senior Leadership, directors and governors are updated by the Head/eSafety co-ordinator and all directors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This purpose of this policy, supported by the Trust and Academy's acceptable use agreements for pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory Trust and school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

ESafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. ESafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- Each school has a strategy for teaching internet skills in Computing and PSHE lessons.
- Each school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modeling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice

or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.

ESafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues in the form of annual briefings each September.
- New staff receive information on this eSafety Policy as part of their induction and are asked to confirm that they have read and will follow it at all times.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All teaching staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

The use of e-mail within schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

E-Mail

The use of e-mail within schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

The Trust gives all staff, governors and directors their own e-mail account to use for all school and Trust business as a work based tool. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The Trust email account should be the account that is used for all Trust and school business

<u>Staff, governors & directors</u>

- Under no circumstances should staff, governors or directors contact pupils or parents with regard to any school business using personal e-mail addresses.
- E-mails created or received by staff, governors or directors as part of their Trust role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail account as follows:
- Delete all e-mails of short-term value.
- Organise e-mail into folders and carry out frequent house-keeping on all folders and

archives.

- Staff, governors & directors must inform the Designated Safeguarding Lead and IT Manager if they receive an offensive e-mail.

Pupils

- Pupils may only use school approved accounts on the school system.
- All pupil e-mail users must ensure that they do not use inappropriate language and do not reveal any personal details about themselves or others in e-mail communication.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing Scheme of Work.

Sending E-Mails

Staff, governors and directors should follow the following guidelines:

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section
-
- E-mailing Personal, Sensitive, Confidential or Classified **Information**.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- When sending e-mails to external organisations, parents or pupils, check the email carefully before sending, in the same way as a letter written on school headed paper. The email must include the senders name and job title. E-mail content should always be polite and tolerant of the views of others and will reflect the standards expected of an employee of Uffculme Academy Trust.
- Do not send or forward attachments and hyperlinks unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- Do not forward chain e-mails, send spam or spoof e-mails containing hoax virus warnings.
- Academy e-mail is not to be used for personal advertising except with the express permission of the Headteacher.
- Consider the timing and likely impact of any email sent outside of working hours and do not expect a reply until working hours resume.

Receiving e-Mails

Staff, governors and directors should follow the following guidelines:

- Check their e-mail regularly including their junk e-mail box as legitimate e-mails (particularly from parents using webmail accounts) may end up there.
- Activate their 'out-of-office' notification when away for more than 4 days.

- Never open attachments from an untrusted source; consult the ICT Support Team first.
- The automatic forwarding and deletion of e-mails is not allowed unless authorised by ICT Support staff.

E-mailing Personal, Sensitive, Confidential or Classified Information

Staff, governors and directors should assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.

If confidential information has to be e-mailed, the following guidelines should be followed:

- Do not send the information to anybody/person whose details staff have been unable to separately verify (usually by phone).
- If emailing to an external recipient then it should be sent as an encrypted document attached to e-mail.
- Provide the encryption key or password by a separate email or ideally an alternative contact for the recipient(s). two email addresses – Gapps uses Virtu
- Request confirmation of safe receipt.
- Do not identify such information in the subject line of any e-mail. – needs re-enforced.
- Do not put a pupils name or initials in the subject line but mark it as CONFIDENTIAL.

Pupils with Additional Needs

The Trust endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the Trusts' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged. Systems are in place to detect and flag inappropriate use. This may be acted on immediately upon detection, and/or if concerns are raised.

Use of the Internet

- Staff must preview any recommended sites before use.
- Any on-line educational resources, which require uploading student details, must have prior approval of the Trust's data Protection Officer.
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material) The Academy filtering system will stop most inappropriate sites but some may slip through.
- In the event that inappropriate material is accidentally accessed it must be reported to a member of the ICT Technical support team immediately.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute Trust software or software from other sources.
- All users must observe copyright of materials from electronic resources including multimedia resources such as You Tube.

Infrastructure

- Our schools also employ some additional web filtering which is the responsibility of the IT Manager.
- Uffculme Academy Trust is aware of its responsibility when monitoring staff communication under current legislation and takes into account; General Data Protection Regulation 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity is monitored and can be accessed if required.

- The Trust does not allow pupils access to internet logs.
- The Trust uses management control tools for controlling and monitoring workstations and logging user activity, including web browsing. This extends to all trust devices whether in school or elsewhere.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the schools, by delegation to the IT Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all Trust machines.
- Pupils and staff are not permitted to download programs on Trust based technologies without seeking prior permission from Subject Leader, teacher or other appropriate adults in school.
- If there are any issues related to viruses or anti-virus software, the IT Manager should be informed.

Student Use of Social Media

The Web, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and (extra space) free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Definitions and Scope
Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Skype, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Ask.fm, Instagram, Snapchat and comment streams on public websites such as newspaper sites.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

- At present, the schools endeavour to deny access to social networking sites to pupils within school.
- Pupils are not allowed to use their mobile phones at all during the Academy Day with the exception of the sixth form and where express permission has been given by a teacher – *see mobile phone policy*.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests).
- Our pupils are advised to set and maintain profiles on such sites to only show their name and profile picture publically and to deny access to any unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

Our pupils are asked to report any incidents of bullying to the school

Staff, Governor & Director Use Of Social Media

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the Trust, the community, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The purpose of this section of the E-Safety Policy is to:

- Protect the Trust and Academy from legal risks.
- Ensure that the reputation of the Trust, the Academy, its staff, Directors and governors is protected.
- Safeguard all children.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

All staff, governors and directors should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and ICT Acceptable Use Policies.

Within this policy there is a distinction between use of school sanctioned social media for professional educational purposes, and personal use of social media.

1. Personal use of social media

- Trust employees, governors and directors must not do anything to risk the safeguarding of pupils within the Trust or to harm the reputation of the school or Trust in any posts, comments or communications on any social media platform
- Any concerns regarding any communication received from children must be reported to the designated person for Child Protection (Deputy Headteacher – Pastoral).
- If any member of staff, governor or director is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Staff, governors and directors should not routinely accept current students as 'friends' except in exceptional circumstances (e.g. close family friends etc.)

- All privacy settings must be set to the highest possible levels on all personal social media accounts.
- Staff, governors and directors are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- This policy must be adhered to at all times including on School trips and when absent from school due to illness etc.
- Staff, governors and Directors will ensure that any online activity outside the Trust will not bring the Trust into disrepute

2. School sanctioned use of social media

There are many legitimate uses of social media within the curriculum and to support student learning.

When using social media for school purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- Staff should not communicate with students via social media.
- The URL and identity of the site should be notified to the appropriate Head of Department or member of the SLT before access is permitted for students.
- The content of any school sanctioned social media site should be solely professional and should reflect well on the school.
- Staff must not publish photographs of children without the written consent of parents / carer's, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe
- Any inappropriate comments on or abuse of school sanctioned social media should immediately be removed and reported to a member of SLT.
- Staff should not engage with any direct messaging of students through social media where the message is not public.

Sexting

Sharing photos and videos online is part of daily life for many young people, enabling them to share their experiences, connect with friends and record their lives. Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps, such as Snapchat, WhatsApp or Facebook Messenger. This increase in the speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to

sexual exploitation. Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is also illegal. This includes imagery of yourself if you are under 18. Although the production of such imagery is most likely to take place outside of school and college, these issues often manifest in school.

The National Police Chiefs Council (NPCC) made clear in 2016 that "incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues". The NSPCC also stated that "Schools should respond to incidents without involving the police provided that the young person shared the imagery consensually and there is no intended malice. Any such cases should be dealt with by the school directly". They went on to say however that incidents should be referred to the Police if there were aggravating factors such as a young person sharing imagery "without consent and with malicious intent".

When an incident involving youth produced sexual imagery comes to the school's attention:

- The incident should be referred to the Designated Safeguarding Lead (DSL) as soon as possible.
- The DSL should hold an initial review meeting with appropriate school staff.
- There should be subsequent interviews with the young people involved, if appropriate.
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

The initial review meeting should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people.
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person. In most cases the imagery should not be viewed.
- What further information is required to decide on the best response.
- Whether the imagery has been shared widely and via what services and/or platforms.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another school, college, setting or individual.
- Whether to contact parents or carer's of the pupils involved - in most cases parents will be involved.

An immediate referral to police and/or children's social care should be made if at this initial stage:

- The incident involves an adult.
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.
- You have reason to believe any pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply then the school may decide to respond to the incident without involving the police or children's social care. The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework.

Searching devices, viewing and deleting imagery

Viewing the imagery

Adults should **never** view youth produced sexual imagery unless there is good and clear reason to do so. The decision to view imagery should be based on the professional judgement of the DSL and should always comply with the safeguarding policy and procedures of the school. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil. If a decision is made to view imagery the DSL would need to be satisfied that viewing is the only way to make a decision about whether to involve other agencies i.e. it is not possible to establish the facts from the young people involved.

If it is necessary to view the imagery then the DSL should:

- Never copy, print or share the imagery; this is illegal.
- Discuss the decision with the Headteacher.
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Headteacher.
- Ensure viewing takes place with another member of staff present in the room, ideally the Headteacher or a member of the senior leadership team. This staff member does not need to view the images.
- Ensure viewing takes place on school or college premises, ideally in the office of the Headteachers or a member of the senior leadership team.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery.

- Record the viewing of the imagery in the school's safeguarding records including who was present, why the image was viewed and any subsequent actions.
- Ensure this is signed and dated.

If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a young person or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school systems) then the DSL should ensure that the staff member is provided with appropriate support. Viewing youth produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

Deletion of images

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for devices, search data on devices and delete youth produced sexual imagery.

The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone has been seized, a senior member of staff who has been formally authorised by the Headteacher can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.

In most cases young people should be asked to delete imagery and to confirm that they have deleted the imagery. In normal circumstances adults should not search through devices and delete imagery unless there is good and clear reason to do so. Young people should be reminded that possession of youth produced sexual imagery is illegal. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the young person. At this point the school may want to invoke their own disciplinary measures to discourage young people from sharing, creating or receiving images but this is at the discretion of the school in line with its own behaviour policies.

Recording incidents

All incidents relating to youth produced sexual imagery must to be recorded either in a safeguarding chronology or in the Sims Behaviour module whichever is most appropriate. This includes incidents that have been referred to external agencies and those that have not.

Teaching young people about sexual imagery

We recognise that teaching about safeguarding issues in the classroom can prevent harm by providing young people with skills, attributes and knowledge to help them navigate risks. Learning about youth produced sexual imagery cannot be taught in isolation. Learning about youth produced sexual imagery will be taught through the PSHE programme, as well as in the school's computing programme of study where it will reflect the requirements of the National Curriculum programme of study for computing. Given the potential sensitivity of these lessons it is essential that this issue is taught within an emotionally safe classroom climate where clear ground rules have been negotiated and established and where boundaries around teacher confidentiality have been clarified. If during any lesson teachers suspect any child or young person is vulnerable or at risk the school's safeguarding protocols should always be followed.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).
- Parents/carers are expected to sign a Home School agreement containing the following statement:
- "Ensure my child understands and signs the School's ICT Acceptable Use Agreement"
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website/Learning Platform postings
    - Newsletter items
    - Learning platform training

Passwords and Password Security

Passwords

Staff, governors and directors should follow the following guidelines:

- Do not use anyone else's logon details to access computer based services
- Change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Never disclose your password to anyone else, with the exception of ICT Support Staff who may, in rare circumstances, request it to provide troubleshooting. This situation will always be avoided if at all possible
- Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff, governors, Directors and pupils who have left the School are removed from the system within one month

  (Users are disabled when they are marked absent in SIMS as this is linked and their emails are removed via an email to SCC, the user account is deleted after 3 months) This is automatically done via RM Network provisioning)

If staff, governors or directors think their password may have been compromised or someone else has become aware of their password the must change it immediately and report it to the ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username.
- Pupils are not allowed to access on-line materials or files on the school network, which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school and Trust networks. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic lock time for the school network is 10 minutes.
- Due consideration should be given when logging into the school online services, such as Cloud, My Learning, Office365 etc. When logging out, they must ensure that they are fully signed out if they are using a shared PC.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the Trust permits the appropriate taking of images by staff and pupils with Trust.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken using these devices provided they are transferred immediately and solely to the secure storage facilities provided via the Academy IT Systems and deleted from the staff device and any storage media.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others without their express consent, this includes when on field trips.

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

---

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site.
- On the school's Learning Platform.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/transmitted on a video or webcam.
- In display material and on electronic displays that may be used in the schools' communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue, eg

divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time.
Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Press Officer, IT Manager and members of the Senior leadership team have authority to upload to the website.

Storage of Images

- Images/films of children are stored on the Trust' secure storage facilities.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platform.

Webcams and CCTV

- Schools within the Trust use CCTV for security and safety. A separate CCTV policy governs this area.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, e.g. monitoring hens' eggs and never using images of children or adults
- Misuse of the webcam by any member of the school community may result in disciplinary action being taken

Trust ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

Trust ICT Equipment

- As a user of ICT, staff are responsible for any activity undertaken on the Trust's ICT equipment provided to them.
- Schools will log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Visitors to the schools should not be allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available.
- Staff should ensure that all ICT equipment that they use is kept physically secure.
- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material) The Trust filtering system will stop most inappropriate sites but some may slip through
- It is imperative that staff save their data on a frequent basis to the Trust's storage system where it will be securely backed up. Staff are responsible for the backup and restoration of any of their data that is not held on the Trust's network drive.
- Personal or sensitive data should not be stored on the local drives. If it is necessary to do so the local drive must be encrypted.
- A time locking screensaver is applied to all machines. Any PCs etc. accessing personal data must have a locking screensaver as must any user profiles.
- Staff must not knowingly project sensitive data on to a screen in a classroom.
- Privately owned ICT equipment should not be used on a Trust network. Without prior approval of the ICT Support team.
- The Trust's IT system must not be used for any non-Trust business or commercial purposes
- On termination of employment, resignation or transfer, staff must return all ICT equipment to their Manager. Staff must also provide details of all their logons to third party systems used by the school so that they can be disabled.
- It is your responsibility to ensure that any information accessed from staff's own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

This section covers such items as laptops, and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on Trust systems and hardware will be monitored in accordance with the general policy
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material) The Trust filtering system will stop most inappropriate sites but some may slip through
- Staff must ensure that all data is stored on the secure storage facilities provided by the Trust's IT systems and that the device is synchronised to these systems on a frequent basis
- Any equipment where personal data is likely to be stored must be encrypted

  (All our windows 10 machines have bit locker available for staff to encrypt drives and portable storage devices)
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- No other user should have access to the 'local login' that has been set up in your name to allow access to the Trust network from outside of work . Nor should you disclose the password to that account. Additional user accounts must be set up for any other person who has access to the device. ICT Support will help with this if necessary.
- Staff are responsible for any damage or inappropriate use of Trust equipment by persons allowed access to it.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied
- Portable equipment must not be used to record meetings unless agreed by all parties present

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices,

mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our schools choose to manage the use of these devices in the following ways so that users exploit them appropriately.

Staff use of Personal Mobile Devices (including phones)

- Staff are responsible for the security of their school mobile phone. They should always set the PIN code on their school mobile phone and must not leave it unattended and on display (especially in vehicles).
- Staff must report the loss or theft of any school mobile phone equipment immediately.
- The staff member will be responsible for all call costs made on a stolen phone until the phone is reported lost or stolen.
- Staff will not attempt to access any sites containing inappropriate (e.g. pornographic, racist, hateful or otherwise offensive) material. This includes viewing, displaying, downloading, printing of such material) The Trust filtering system will stop most inappropriate sites but some may slip through.
- Staff must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it.
- School SIM cards must only be used in school provided mobile phones without prior approval from ICT Support.
- Staff must not send text messages to premium rate services.
- Staff must never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.
- When overseas, data roaming should be turned off and only switched on for brief periods if no WiFi is available.
- The Trust allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/carer using their personal device.
- The Trust is not responsible for the loss, damage or theft of any personal mobile device.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- The sending of inappropriate communications between any member of the school community is not allowed
- Mobile phones must not be used to record meetings unless agreed by all parties present
- Staff must not have their mobile phones out during the school day in front of the students

Pupil use of Personal Mobile Devices (including phones)

- Pupils are allowed to bring personal mobile devices/phones to school but only if they are switched off at all times within the school day and are in their bags or coats.
- This technology may be used, however for educational purposes under the express permission of the class teacher. The device user, in this instance, must always ask the prior permission of the bill payer
- Mobile phones cannot be used at break or lunchtime.
- The Academy is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate communications between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Mobile phones must not be used to record meetings unless agreed by all parties present
- 6th form students can only use their mobile phones in the **6th form block**

Removable Media

- Due to the accessibility of the secure storage facilities provided via the Trust's IT Systems there should be no requirement to routinely store any school data on removable media.
- If circumstances do require the use of removable media, there must be no sensitive or confidential information stored on it, unless the media is encrypted.
- Users must be aware that data on removable media is not backed up and any data loss will likely be irreversible.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

There will be an on-going opportunity for staff to discuss with either the IT Manager or the Designated Safeguarding Lead any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change

the orders or guidance in any way.

Current Legislation

Acts Relating to Monitoring of Staff eMail

General Data Protection Regulation 2018

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This

wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his

course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

General Data Protection Regulation

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Appendix 1

Acceptable Use of the School's IT System and the Internet (by Students)

The school's IT system (inc access to the Internet, e-mail and other digital resources) are there to support your learning. To help keep you safe and everyone else safe and to ensure that you make use of these resources in a way that is appropriate and legal the following rules have been put in place. Please read them carefully and if there is anything you don't understand, please ask your tutor or ICT teacher.

I agree that:

- I will never share my password with anyone or use anyone else's password. If I become aware that my own password has become known to someone else, or I find out someone's password I will immediately inform the ICT Technical Support Team
- I will never infringe the security or privacy of another user. I will never attempt to access or alter their files or folders, or tamper with their storage area on the school system or any removable media (e.g. flash drive) they may have.
- I will do everything I can to keep myself and others safe on the Internet. I will never disclose or publicise personal information about myself or others (e.g. home address or telephone / mobile number), nor will I respond to requests using SMS or agree to meet with someone.
- I will always treat other IT users with respect and will never harass, threaten, harm, insult or offend them.
- During lessons, I will only use the school's IT systems and equipment for educational purposes linked to the learning objectives of the lesson. At break and lunchtimes students I may use the facilities for personal purposes provided they meet the other sections of the policy
- I will take care of all IT equipment and the IT environment and I will not remove any IT equipment from its current location, either temporarily or permanently.
- I will not download or bring into school unauthorised programs, or attempt to install or store them on the school's IT system or on any of its equipment.
- I will never knowingly introduce a virus or other malware to the school's systems
- I will not access or download inappropriate (e.g. pornographic, racist or offensive) materials and will ensure that none of my files contains such material. This

includes viewing, displaying, downloading, and printing, sending, or otherwise transmitting materials.

- I will switch off or close my screen immediately and report to a teacher if I discover an unsuitable site.
- I will not access Internet chat rooms, social media websites, or messaging services (inc chat sites) using the school's system. I will not access online games sites during lessons
- I am aware of the 'Report It' button and know when to use it.
- I will not make audio or video recordings of another student or member of staff without their permission.
- I will never send or forward inappropriate images of myself (or others) to another person and understand that to do so is criminal offence.
- I will not copy information into assignments without fully acknowledging the source of it. I understand that if I break this rule it could be classed as plagiarism and/or copyright infringement and so have serious consequences, particularly where the work is being submitted for exam purposes.
- I will not copy or distribute any copyrighted material (inc software, video, music etc.) and understand that it is illegal to do so.
- I will only use my school email account for school work and school related activities. When writing, or replying to emails I will always be polite towards others and tolerant of their views in what I say. The same applies to any attachments I may send.
- I will only open emails (and any attachments) if they come from someone I already know and trust.
- I will not forward chain e-mails, send spam or spoof e-mails or e-mails containing hoax virus warnings.
- Staff may review my files and communications (inc. e-mails) where there are concerns about the content and/or to ensure that the system, equipment and other media are being used responsibly. This may include random checks.

Please remember that if you act in an inappropriate manner your access rights may be withdrawn, which would adversely affect your learning, and further sanctions may also be imposed.

Acceptance of the above conditions:

Full Name: _____Tutor Group: _____

Signature: _____Date: _____

Parent's Signature: _____