*e*safety policy

APRIL 2012

Hall Cross Academy

Date Approved:	23rd April 2017
By Whom:	Health & Safety Committee
Review Date:	August 2018
Responsible Officer:	Siân Stockham

Hall Cross Academy 2017/2018

The following document has been adapted from the Internet Policy document produced by Doncaster LA and includes sections taken from the Becta Website and reproduced under the Open Government Licence.

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the Academy Development Plan (Section 4) and relates to other policies including those for ICT (AUPs), Behaviour, Bullying and for Safeguarding.

The people responsible for e-safety at Hall Cross Academy are the Designated Safeguarding Leads.

This is James Harris and Siân Stockham.

- The Governor responsible for e-safety is Mr David Cox
- This e-Safety Policy has been written by the academy, building on the Doncaster e-Safety Policy and government guidance. It has been reviewed and amended in September 2017. It has been agreed by senior management and approved by Academy Trustees
- The e-Safety Policy was revised by Siân Stockham

The next review date is August 2018.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business, leisure and social interaction. The academy has a duty to provide students with high quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.
- Internet use will enhance and extend learning
- Hall Cross Academy Internet access is designed expressly for student use and includes differentiated filtering appropriate to the age/curriculum of students.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and this is discussed with staff and students. Training and guidance for staff takes place in annual safeguarding training and regular bulletins. Training for students takes place through lessons and assemblies.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This is part of the Baccalaureate curriculum in Y7 & 8, the ICT/Computer Science curriculum in Y9 and Life lesson in Y10 & 11.

Students are taught how to evaluate and review Internet content

Evaluation of online resources is important – it can help to determine the reliability, accuracy and currency of the material found on the internet. Teachers will critically evaluate websites when selecting resources for use in the classroom, and students will

also be taught these skills as part of their digital literacy skills development across the curriculum. (Appendix 1)

Copyright and Online Content

Hall Cross Academy endeavours to ensure that the use of Internet derived materials by staff and by students complies with copyright law. (Appendix 2)

Plagiarism

Plagiarism is cheating and may constitute a criminal offence by breaching the copyright laws.

Plagiarism is a particular issue in educational settings. Plagiarism is the theft of ideas and works from another author and passing them off as one's own. It is not a new phenomenon but the advent of digital technologies, and the growing philosophy of sharing information across the internet, has made such theft far easier to perform and possibly more difficult to uncover. Hall Cross Academy discourages plagiarism and deals with proven instances severely and appropriately.

Ofqual have produced the following guides on plagiarism:

- Authenticity: A Guide For Teachers
- Using Resources: A Guide For Students: Find It – Check It – Credit It
- Avoiding Plagiarism: A Guide For Parents And Carers

Managing Internet Access

Information system security

- Hall Cross Academy's ICT system security will be reviewed regularly by the Assistant Head and security strategies will be discussed at least annually by the Senior Leadership Team.
- Virus protection is installed and updated regularly. The Academy currently uses Sophos as its anti virus protection.
- The academy uses the e-safety monitoring software Securus. Parents and students are made aware of this in the Acceptable Use Policies. If an inappropriate word appears in a pupil's e-mail, or work, a report is produced and violations result in letters being sent home and students' internet and e-mail accounts being reviewed
- Each Key Stage is monitored using Securus and staff usernames are also monitored
- Security strategies are discussed at ICT Strategy and Safeguarding Strategy meetings
- Data security policy is reviewed by the ICT strategy group (Appendix 4)
- Smoothwall is used as the network filtering software

E-mail

- Students and staff may only use approved e-mail accounts on the academy system. Students must immediately tell a member of staff if they receive offensive e-mail
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- Students are taught e-mail etiquette, including how e-mail from students to external bodies is presented and controlled
- Training for staff and students includes explicit reference to only using Academy email systems for communication between each other

Cyberbullying

Children and young people are keen users of new technology, but this can also leave them open to increased risks from bullying by text message, email or online via websites and social networking sites. This type of bullying is called online bullying or cyberbullying.

Effective education, and awareness of the issues, can help to reduce the risks and provide an open culture where bullying of this nature can be freely reported and discussed, whether it takes place in academy or elsewhere.

- Any incident of cyberbullying should be dealt with in accordance with the academy's Safeguarding policy
- Anti-bullying statements are also incorporated in the acceptable use policy (AUP)

Staff may also become targets of cyberbullying. Any incidence should be reported immediately to the DSL.

The guidance, "Cyberbullying: Supporting academy staff" (http://www.teachernet.gov.uk/wholeacademy/ behaviour/cyber), provides further information on this issue, including protecting personal information and getting offensive online content taken down.

Published content and the academy web site

The academy website is a great way of promoting all the good work that goes on in academy to both current and prospective members of the academy community.

The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

- The Vice Principal has overall responsibility for the academy website
- Staff or student personal contact information is not published. The contact details given online are for the academy office.

- Website content is regularly reviewed to ensure that it remains current and does not compromise student or staff safety, and its content does not infringe the intellectual property rights of others.
- All staff members with administrative rights to the school website will be trained in e-safety risks, personal information risks, data protection and copyright risks

Publishing students' images and work

Written permission from parents or carers is obtained when students join the academy before photographs of students are published on the academy website or in any other medium.

Parents/Carers are advised that:

- The academy will not use the personal details (e.g. address, phone number etc) of any child or adult in a photographic image or video, on our website, in the academy prospectus or in any other printed publications
- The academy will not publish the name with any photographs of students in external publications and/or publicity releases without the explicit permission of parents/carers (for example when celebrating sporting or academic success)
- The academy may use a pupil's name and photograph in academy magazines and other internal publications celebrating pupil success, and ensure that students are suitably dressed to reduce the risk of inappropriate attention
- The academy may include pictures of students and teachers that have been drawn by students
- The academy may use group or class photographs or footage with very general labels such as "science lesson" or "making Christmas decorations"
- The academy will only use images of students who are suitably dressed, to reduce the risk of such images being used inappropriately
- The academy will ensure that videos don't inadvertently contain personal details, for example in voiceovers or credits
- The academy will ensure that image and video files are appropriately stored and named on the academy network

Social networking and personal publishing

Whilst it is accepted that social networking is an integral part of most people's lives, most social networking sites have minimum age restrictions. As a result access to some social networking sites is not permitted in the academy. The Academy recognises the benefits to learning of social media and will empower the students with the knowledge to use it safely and appropriately. Additionally:

- Newsgroups are blocked unless a specific use is approved
- Students are taught never to give out personal details of any kind which may identify them, their friends or their location
- Students are told never to meet with a 'friend' that they have only ever met via a social networking site
- Students are told not to place personal photos on any social network space without considering how the photo could be used now or in the future
- Students are advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications
- Students are advised to only invite known friends and deny access to others

- Staff that use social networking sites are told to ensure that they have set their privacy settings appropriately and that they should never publish images that contain any students of the academy. Training for staff (where social networking sites will be unblocked) will be provided as part of the regular CPD cycle in school to ensure that all colleagues are well informed. "Surgeries" are arranged for staff to have their social media settings checked, if they wish
- Staff that use social networking sites must be mindful of any comments they publish that could bring the Academy into disrepute; referenced within AUP

Managing filtering

- The academy uses Smoothwall for internet filtering
- The academy will ensure that systems to protect students are reviewed and improved whenever any changes to Academy ICT provision are planned
- If staff or students discover a website considered to be age or curriculum inappropriate, it must be reported to the DSL or the Systems Manager
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Requests to have websites unblocked will be submitted to the Systems Manager. The Systems Manager and DSL will assess the website and only when all members of the panel agree that the site is acceptable will the site be unblocked

Mobile and Emerging Technologies

Developments in mobile technology have been rapid in recent years, meaning that mobile phones (and other personal devices) can now do much more than make voice calls. Integrated cameras, video messaging, mobile access to the internet, cloud-based services and location-based services are now commonplace, allowing access to a whole array of new content and services. (Appendix 5)

Children and young people have always been keen to grasp the opportunities offered by new technology and, with increasing rates of ownership at an ever lower age, mobile phones are no exception. However, as with any technology, there are associated risks: children and young people need to understand the issues, and develop appropriate strategies and behaviours, for keeping themselves safe.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in academy is allowed.

Although technology, when applied in a safe and managed way, can enhance learning and bring lessons to life for the benefit of learners, caution is advised if using mobile phones (and other personal devices) in an educational setting. To this end, following a review the use of Mobiles technologies is now allowed in line with the Mobile Device policy (Appendix 6). Students will be permitted to use mobile devices in lessons, given the permission of the

staff member and will be permitted to access the internet using the Academy wireless network which is subject to the same filtering policies as the hard-wired network.

The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass academy filtering systems and present a new route to undesirable material and communications.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff AUP' (Appendix 7) annually before using any academy ICT resource. They should be aware of the Hall Cross Academy Professionalism in Practice Policy. (Appendix 8) At the start of each academic year a flash screen will force all members of staff to accept these policies if they wish to access network resources. This will follow the annual training around e-safety expectations that takes place as part of the annual safeguarding (KCSIE) training for all staff members.

- The academy will maintain a current record of all staff and students who are granted access to academy ICT systems.

- Students receive the Student Acceptable Use Policy (Appendix 9) when they join the academy. Compliance to this is managed through the use of an esafety lesson at the beginning of the year which outlines the responsibilities for all in the AUP and a subsequent digital signature on sign-in.

Assessing risks

The academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the academy network. The academy cannot accept liability for any material accessed, or any consequences of Internet access but will take all reasonable endeavours to prevent any wrongdoing.

The DSL will regularly audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate and effective.

Securing and preserving evidence if illegal online activity is suspected

Care must be taken to secure and preserve evidence if illegal online activity is suspected on the academy network, or involves a member of the academy community, be that staff or students.

On academy premises

- Following any incident that may indicate that evidence of indecent images or offences concerning child protection may be contained on academy or college computers, the matter should be referred to the Headteacher who should in turn notify police at the earliest opportunity.
- Suspect computers will not be used or viewed until authorised by the police hi-tech crime unit.
    - There are many instances where academies or colleges, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have become aware of raised suspicions. In some circumstances this interference with evidence may constitute a criminal offence also
    - The police will be interested in obtaining 'best evidence'. This, in reality, will be to forensically copy computers that may contain evidence of offences. This can be carried out discreetly out of hours, having minimal impact on the Academy
- For further information see the Internet Watch Foundation best practice guide on handling potentially illegal images of children.

On home computers

- If a pupil or staff member discloses potential crimes involving computer-based media, again the police will normally try to obtain a forensic copy of their home computer to preserve any evidence. This will be conducted discreetly and, in many cases, the computer will be returned quickly. However, the point must be made that the impact on the family of the pupil or staff member could have far-reaching consequences should illegal material be suspected or discovered. The academy will ensure that appropriate support mechanisms exist if such a situation should occur.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a DSL
- Any complaint about staff misuse must be referred to the Headteacher, as with other safeguarding concerns
- Complaints of a safeguarding nature will be dealt with in accordance with Academy safeguarding procedures.

The academy has an anti-bulling policy and a 'Bully Button'. This is an e-mail system for students to report any form of Bullying. This is entirely confidential. All e-mails go directly to the DSL who forwards these to Heads of Year. The HOY will decide on appropriate action. A record of all reported bullying is kept by the DSL as part of the whole school safeguarding logs.

Communicating e-Safety

Introducing the e-Safety Policy to students

- A number of books on e-safety are available in both the Upper and Lower site library
- Students are informed that network and Internet use is monitored using Securus.
- e-Safety is incorporated into Y7 & 8 Bacc lessons, Y9 ICT lessons and Y10-11 Life lessons as well as through regular assemblies
- Whole school lessons are planned and delivered to ensure students understand the AUP and the consequences of not complying with this

Staff and the e-Safety Policy

All staff will be given the Academy e-Safety Policy and its importance explained.

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the Academy e-Safety Policy on the Academy website and in admissions packs
- The academy will maintain a list of e-Safety resources for parents/carers and these will be made readily available on the Academy website. This includes regularly updated newsletters and advice and guidance for parents

Appendix 1 – Evaluating Online Resources

When evaluating online resources, the following should be considered:

Accuracy and currency

- Does the information appear to be accurate?
- Is it based on opinion or fact?
- Are additional references given?
- Can the information be verified from other sources, whether online or hard copy?
- Is the spelling and grammar correct?
- Is the content dated?
- When was the content last updated?
- Do all the links work?
- Are any areas of the site incomplete or 'under construction'?

Authority and coverage

- Does the content have authority?
- Where does the content originate from?
- Who is the author or publisher of the site?
- Are they qualified to provide information on this topic?
- Is the material biased?
- Can the author/site owner be contacted?
- Where is the content published? What is the domain name of the website? Is it published by a large organisation, or on a personal website?
- Does the website cover the topic fully?
- Does the site provide information/advice/ideas/other choices?
- Does the content provide links and references to other materials?
- If links to other materials are provided, are these evaluated or annotated to provide further information?
- Does the site contain any advertising? If so, does it influence the content?

Audience and relevance

- Who is the intended audience for this content?
- Is the content easy to read and understand?
- Is the site specifically aimed at children? If so, is the level and tone of the content appropriate?
- Is the site specifically aimed at adults? If so, beware of inappropriate material.
- Is the content relevant?
- Does the material provide everything that is needed?
- Could more relevant material be found elsewhere, for example in a book or magazine?

Educational focus

- Is there an obvious educational focus to the content?
- Will it support learners with different learning styles? How does it use media to support people with auditory, visual, kinaesthetic or other learning preferences?
- Does it have links, or refer to, the appropriate stages of the National Curriculum or exam syllabus?

Ease of use

- Is the site easy to use?

- Is it well structured?
- Is it easy to find relevant information?
- Is the content in an easy-to-use format?
- What facilities does the site provide to help locate information?
- Does it have a search facility? Is the menu navigation logical? Does it provide a site map or index?
- Does the site load quickly?
- Is the site attractive in design?
- Is the content copyright, or can it be used elsewhere providing the source is acknowledged?
- Is the site technically stable?

Appendix 2 – Copyright

In basic terms, copyright gives the creators of materials control over how they are used. Copyright protection comes into force as soon as something is created or fixed in some way; whether that is on paper, film, in audio format or electronically such as a website, CD-ROM or database. Copyright does not, however, protect ideas, names or titles.

Legislation

Copyright law in the UK is outlined in Part I of the Copyright, Designs and Patents Act 1988 which has been updated by various legislation over the years. It was most recently amended by The Copyright and Related Rights Regulations 2003 (SI 2003, No. 2498).

Whereas the original focus of the legislation was on making copies of printed resources, subsequent amendments to the Act also govern the use of other media, including new and emerging technologies.

To support visually impaired users, the Copyright (Visually Impaired Persons) Act 2002 allows copying of hard copy and digital materials to create an accessible format. This might allow, for example, texts to be copied and enlarged for use with access devices. Further information is available on the RNIB website.

Copyright and online content

Under UK law, copyright material published on the internet will generally be protected in the same way as material in other media. Furthermore, each web page may contain several different copyrights if it contains text, music, graphics and so on.
While there are no specific exceptions to copyright material on the internet, many of the exceptions applying to hard-copy materials might also apply. For example fair dealing provision allows for a single copy of a page for the purposes of non-commercial research or private study.

Many websites will include a copyright statement setting out exactly the way in which materials on the site may be used. When using websites in educational settings, students should be encouraged to look for copyright information, so reinforcing their understanding of the importance of this issue.

Students should also be aware that many online resources may have been published illegally without the permission of the copyright owners. This may be particularly the case with media-based content such as music and videos. Any subsequent use of the materials may also be illegal. Childnet International provide useful guidance on Young people, music and the internet, while the Pro-Music website provides information and news about legitimate music online.

Remember also that copyright law differs in other countries, which may be particularly relevant if using websites which have been created or are hosted overseas.

Helpful resources on intellectual property and copyright

British Copyright Council

The British Copyright Council (BCC) is a national consultative and advisory body representing organisations of copyright owners and performers, and others interested in copyright in the UK.

Creative Commons

The Creative Commons website gives advice on copyright for work published online, allowing work to be copied and distributed under the conditions specified by the originator.

Digizen

The Digizen website provides information for educators, parents, carers, and young people. It is used to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible digital citizens. It includes a section on digital values, including copyright and plagiarism.

Institute for Citizenship

The Institute for Citizenship, through its education work, supports teachers to interpret the citizenship curriculum. It provides a range of teaching resources including a free interactive CD-ROM produced in association with the UK Patent Office. Aimed at Key Stage 4 students, Net Benefit focuses on the use of the internet from a consumer perspective, including information on copyright law.

Intellectual Property Office

This site acts as a signposting resource for information on intellectual property, and provides specific information on intellectual property in education and online.

Teachernet

This website gives an overview of copyright specifically for teachers, including issues relating to radio, television and the internet.

Copyright licensing organisations

Christian Copyright Licensing International

Christian Copyright Licensing International (CCLI) licenses academys for use of copyright materials for collective worship. The licence includes making songsheets and songbooks, inputting lyrics into a computer, making presentation slides and recording worship services.

Copyright Licensing Agency

The Copyright Licensing Agency (CLA) is a non-profit organisation which licenses the copying of extracts from books, journals and magazines protected by copyright. Specific guidance for education covers a range of digital technologies, such as interactive whiteboards, VLEs (virtual learning environments), and e-books and e-journals.

Educational Recording Agency

The Educational Recording Agency (ERA) licenses educational establishments to record broadcast materials (such as radio, television and cable programmes) for educational purposes, and allows electronic communication of licensed recordings within an educational establishment. They also

offer the ERA Plus Licence which allows students and teachers to access licensed ERA recordings online, whether they are on the premises of their educational establishment or working elsewhere within the UK.

PRS for Music

PRS for Music collects and distributes royalties to music writers, composers and publishers, generated from the recording and performance or broadcast of music in many different formats. This may be relevant to academys if creating multimedia resources incorporating music, and will also apply to recordings of academy concerts, plays or other events.

Music Publishers Association

The Music Publishers Association (MPA) exists to safeguard and promote the interests of music publishers and writers. They provide a guide to copyright licensing in academys outlining the types of musical activities that need to be licensed.

Newspaper Licensing Agency

The Newspaper Licensing Agency (NLA) licenses organisations to take legal copies of national and regional newspaper articles in both paper and digital formats. Specific information is provided for academys.

Phonographic Performance Ltd

Phonographic Performance Ltd (PPL) is a music industry organisation which collects and distributes airplay and public performance royalties in the UK on behalf of record companies and performers.

UK Music

The UK Music is an umbrella organisation representing the collective interests of the UK's commercial music industry. Specific information is provided for education, along with the SoundRights resource – a free online learning resource to help young people understand the business of music.

Appendix 3 – Data Protection Act: Photographs and Videos

Data Protection Good Practice Note: Taking Photographs in Academies

This Good Practice Guidance is aimed at Local Education Authorities and those working within academies, colleges and universities. It gives advice on taking photographs in educational institutions and whether doing so must comply with the Data Protection Act 1998.

Recommended Good Practice

The Data Protection Act is unlikely to apply in many cases where photographs are taken in academies and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official academy use may be covered by the Act and students and students should be advised why they are being taken.
- Photos taken purely for personal use are exempt from the Act.

Examples

Personal use:

- A parent takes a photograph of their child and some friends taking part in the academy Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Grandparents are invited to the academy nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official academy use:

- Photographs of students or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of students are photographed during a science lesson and the photo is to be used in the academy prospectus. This is unlikely to be personal data and the Act wouldn't apply.

Media use:

- A photograph is taken by a local newspaper of an academy awards ceremony. As long as the academy has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act

Further Information

If you require any further information about this or any other aspect of Data Protection, please contact:
Web: www.ico.gov.uk Email: mail@ico.gsi.gov.uk Telephone: 01625 545700

Appendix 4. Data security policy

The purpose of this document is to define the acceptable use of School ICT systems.

Key terms are defined/explained in the glossary that appears at the end of this document.

This policy forms part of the group of policies covering acceptable use and security of all ICT systems and equipment.

The objectives of the policy, which is intended for all school staff, including governors, who use or support the school's ICT systems or data are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

This policy applies to all staff who use school computing resources and to all uses of those resources, whether on site or from remote locations and forms part of the conditions of employment for staff, and is part of the contractual agreement for suppliers. All parties must read the policy completely and confirm that they understand the contents of the policy and agree to abide by it.

Please note that this policy document has been developed with your personal and professional judgment in mind, either in the classroom or an office environment. It is not intended to cover every eventuality, but seeks to provide guidance on acceptable practice.

1. General Responsibilities

- Users of the schools ICT systems and data must comply with the requirements of the Data Security Policy
- Users are responsible for notifying the Help Desk of any suspected or actual breach of ICT security. The Help Desk will then notify the SIRO who will decide whether to inform the Headteacher. The Headteacher will decide whether to inform the Chair of Governors or the LA.
- Users must comply with the Data Protection Act 1998
- Users must be supplied with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

2. Summary of Individual Responsibility

- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely for storage in a secure location. Users must refer to the instructions for use of the school's chosen encryption software.
- Users must protect all portable and mobile devices, including media used to store and transmit personal information using approved encryption software.
- Users must securely delete sensitive or personal data when it is no longer required.
- Users of school computing resources must comply with national laws, school rules and policies, and the terms of applicable contracts including software licenses. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, the data protection act and computer misuse act.
- Users who engage in electronic communications with persons in other countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.
- Users are responsible for ascertaining what authorisations are necessary and for obtaining them before using school computing resources. Users are responsible for any activity originating from their accounts, which they can reasonably be expected to control. Persons other than those to whom they have been assigned by the Network Manager may not, under any circumstances, use accounts and passwords not issued to them. In cases when unauthorised use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate system administrator.
- Users must not use computing resources to gain unauthorised access to remote computers or to impair or damage the operations of computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or 'sniffing' communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.
- Users should seek permission from the relevant Information Asset Owner before removing any sensitive data from the school.

3. Physical Security

- ✓ As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data
- ✓ Server rooms must be kept locked when unattended
- ✓ Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- ✓ All school owned ICT equipment and software should be recorded and an inventory maintained.
- ✓ Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- ✓ Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons

- × Do not leave sensitive or personal data on printers, computer monitors or desks whilst away from your desk or computer.
- × Do not give out sensitive information unless the recipient is authorised to receive it.
- × Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.
- × Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

4. System Security

- ✓ The System Manager together with the ICT Strategy Group will determine the level of password control.
- ✓ Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- × Passwords should not be revealed to unauthorised persons
- × Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data
- ✓ Passwords should be changed every 60 days – this should be an automatic procedure
- ✓ Passwords must be changed if it is a suspected breach or actual breach of security, e.g. when a password may be known by an unauthorised person
- ✓ Regular backups of data, in accordance with the recommended backup strategy, must be maintained
- ✓ Security copies should be regularly tested to ensure they enable data restoration in the event of system failure
- ✓ Security copies should be clearly marked and stored in a fireproof location and/or off site.
- ✓ Any computer containing personal/sensitive data should be protected by an up-to-date antivirus program.
- ✓ Any computer containing personal/sensitive data should only be able to access the internet through a properly maintained firewall.

5. Use of Data

- All users accessing school data must do so only in conformance to this policy. Data may only be accessed by uniquely identified, authenticated and authorized users.
- Each user must ensure that Hall Cross School data assets under their direction or control are properly labelled and safeguarded according to their sensitivity and criticality.
- Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

6. Data Ownership

All systems will have a system owner, who will take responsibility for the ownership of every system that the School owns or operates. The system owner, in conjunction with the SIRO (see section 8), will define the security requirements for each system.

7. Document handling, storage and transfer

This guidance applies to the access to, storage, transmission and destruction of all personal data, both paper-based and electronic and it is recommended that these steps be followed/adopted.

Document storage

- Different levels of access must be given to directories and these must be clearly identified with Impact Levels.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Sensitive or personal data must be securely deleted when it is no longer required.
- All paper based protected data must have a header and footer printed on each page containing the Impact Level and Classification in the header and the Release and Destruction marking in the footer. (Appendix B)
- All IL2-Protect and IL3-Restricted printed material must be held in a lockable storage area or cabinet. (Appendix B)
- Materials at IL4 and above will not be handled within school.

Document access

- Users are assigned a clearance that will determine which files are accessible to them.
- When data access is required by an authorised user from outside the school premises (for example, by a teacher working from their home) they must have secure remote access to the schools internal network.
- All staff accessing data must have CRB clearance
- SIMS data cannot be currently accessed remotely.

Document transfer

- The act of transferring data will require security policies to be enforced by each system to ensure that only particular data flows are allowed.
- Users may not remove or copy sensitive or personal data from the school or authorised premises unless the media is encrypted and is transported securely and stored in a secure location.

Document Destruction

- Protected data at IL2 or above, in either paper or electronic form, must be disposed of in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten (at least seven times) before being destroyed and other media must be shredded, incinerated or otherwise disintegrated.

Printed Documents

- Printed documents require labels that appear on each page of protected data, in the header and footer. (See Appendix B). Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which are in descending order of sensitivity: TOP SECRET,

SECRET, CONFIDENTIAL, RESTRICTED AND PROTECT. Most learner and staff personal data that is used within school will come under PROTECT.

8. Key Roles and Responsibilities

8.1 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO – Mr M Swift) is a senior member of staff who is familiar with information risks and the organisation's response. The SIRO has the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs)
- They act as an advocate for information risk management.

The Office of Public Sector Information has produced Managing Information Risk [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

8.2 Information Asset Owner (IAO)

Identified information assets include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence. The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations.

An information asset is regarded as the collection of data or an entire data set. It is important to distinguish between an information asset and the information (usually a subset of the asset) that needs protecting. For example, reports run from a core information asset, such as a management information system, are not information assets themselves.

Information Assess Owners (IAO) have been identified as members of the ICT Strategy Group. Each member of the group will take ownership of the identified information assets as deemed appropriate by the SIRO and the group.

The role of an IAO is to understand:

- what information is held, and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off.

It is the responsibility of the IAO to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although we have explicitly identified these roles, the handling of secured data is everyone's responsibility – whether an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

9. Data Back-Up And Recovery Procedure

The following backup procedure will be undertaken by a member of the ICT Technical Support Team. It is also a requirement that all staff ensure the security and maintain backups of their own data, when stored on a laptop or other portable device.

- **Daily incremental backups**. User Data and the SIMS server will have a daily incremental backup. All user data and SIMS data is backed up to disk.
- **Weekly**. A full backup of both User Data and SIMS are backed up to lower school on a weekly basis.
- **Monthly**. A full backup of both User Data and SIMS are backed up to removable disk and stored in a fire proof safe.
- **End of Year**. A full backup of both User Data and SIMS are backed up to removable disk and stored in a fire proof safe for archive purposes.

- **NOTE:** The weekly backups to lower school are in place to maintain an additional off-site safe guard in the event of a catastrophic failure (for example, a major fire that destroys both server locations in the main Upper School Site).

The following section explains your responsibility to back-up the information on your computer in order to avoid losing it.

Your situation	**Back Up Procedure**
Your use of a computer on the network	ICT Technical Support will back up data stored in your personal workspace and designated shared areas on the network.
Your computer is not on the network or you store information on the hard disk or C: drive of your computer	It is your responsibility to regularly save your information on an external storage device and ensure that all sensitive data is encrypted and password protected.(e.g. CD, DVD, USB Storage Device etc.).

10. Encryption and SIMS access

The Information Commissioner's Office recommends that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Any data that may be deemed sensitive, or used to identify an individual (staff or student) must be encrypted if it is to be moved off site.

All staff requiring access to SIMS data will be provided with secure access via the Sims Learning Gateway.

Staff are supplied with an encrypted USB memory stick on request. Staff are instructed to use this encrypted USB memory stick when transferring any data covered by this policy from one computer to another, or offsite.

11. Managing Systems For Staff Leaving

When an employee terminates their employment with the School, the guidelines below should be followed:

- Immediately change or remove the passwords for those user ids to which an employee leaving the School has had access or update capabilities. This standard practice serves to protect the employee in the event of any problems and the School systems against possible tampering. This will be undertaken by ICT Technical Support notification from the Personnel Department.
- The Head of Department will ensure that any data relevant to the operation of the department is transferred from the folder of the member of staff who has left to a departmental shared area.
- When an employee's termination is processed by Personnel, ICT Technical Support will be notified and the user id will be suspended.
- New employees will be provided with a copy of this policy.

12. Managing Systems For Pupil Leavers

When a pupil leaves the School, the guidelines below should be followed:

- Data Manager, Senior Admin Officer (6th Form) or Senior Admin Officer (Lower School) to notify ICT Technical Support when pupils leave
- Immediate suspension of the user id. This standard practice serves to protect the pupil in the event of any problems and the School systems against possible tampering.
- Delete all pupil content from system when pupil leaves, an archive will be kept to allow data to be restored for returning pupils. This archive will be kept for approximately 10 years.
- Each pupil to be responsible for taking a copy of their data.

13. Audit logging and incident handling

- Access to personal/secure data should be logged
- A log of any breach of the data security policy should be kept.
- Information on what data is logged should be clearly defined for staff and students

Appendix A

The Data Protection Act 1998

This came into force on the 1 March 2000. The purpose of the act is to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

The Act applies to personal data (information that applies to a living person) whether it is held on a computer system or on paper. There are particularly stringent rules surrounding 'sensitive' data such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and criminal offences.

Personal data can only be processed under one or more of the following rules:

- An individual has given consent
- It is part of a contract
- It is a legal obligation
- It is necessary to protect the individual
- It is in the legitimate interests of the data controller

Every item of personal data that is held or processed must be accurate and up to date, and held for no longer than necessary. When data is no longer relevant to the purpose for which it was originally obtained, and/or has reached the end of the period for which it must legally be retained, it must be destroyed in accordance with the relevant Impact Level of the data.

The security of personal information must be maintained and any disclosure of personal data must be properly authorised. There are specific consent requirements in respect of data transferred to countries outside the European Economic Area.

It is a legal requirement to protect sensitive data. Individuals entrusted with protected data, however derived, are accountable for the protection and compliance with the laws. This is enforceable through local human resource processes and failure to comply may be construed as gross misconduct and could face prosecution.

Appendix B

Protective Marking

Identifying sensitive or personal data and assessing its impact level

Impact Levels

All data electronic or paper should be labelled according to the protection it requires, based onthese Impact Levels.

The following table illustrates the assignation of Impact Levels for Distress to the Public.

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
None	Likely to cause embarrassment to an individual or organisation	Likely to cause loss of reputation to an individual organisation	Likely to cause embarrassment or loss of reputation to many citizens or organisations	Likely to cause long term (eg months) or permanent loss of reputation to many citizens or organisations	Likely to cause major long term damage to the UK population

Data in schools is protected as generally classified as either IL2 – Protect or IL3 Restricted. The vast majority of typical schools MIS reports or teacher access is to data that is protected at IL3 – Restricted Level.

It is recommended that educational ICT systems are set up to label the output of any protected data as IL3 – Restricted by default.

All documents that contain protected data must be labelled as such with clear handling notes.

Becta recommends a clear method of showing the labels that are applicable in schools and should be placed in the header within documentation.

Release/destruction markings

Becta recommends in order that protected data is securely deleted or destroyed that it should be marked within the footer as below.

Release	Parties	Restrictions	Encrypt, Securely delete or shred
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document should be destroyed
Examples			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information father ASBO	Securely delete or shred

Recommendation and Requirements

- All paper based protected data must have a header and footer printed on each page containing the Impact Level and Classification in the header and the Release and Destruction marking in the footer.
- IL2-Protect and IL3-Restricted material must be encrypted if the material is to be removed, or accessed remotely, from the school.
- All IL2-Protect and IL3-Restricted printed material must be held in a lockable storage area or cabinet.
- Protected data at IL2 or above, in either paper or electronic form, must be disposed of in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten (at least seven times) and other media must be shredded, incinerated or otherwise disintegrated.

Glossary

Antivirus Program	A utility that searches storage devices for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.
Backup	To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails.
Data	Any information that is stored either digitally or in printed/written format and maybe/is used to identify any individual or group, or may be deemed to be sensitive in nature.
Data Protection Act 1998	Legislation that defines how data should be treated, used and stored. See http://www.legislation.org.uk/index.htm for further details
Data Security Policy	This document
Electronic communication	Communication which is transferred electronically
Encryption	A process which is applied to text messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it.
Encryption Software	Software whose main task is encryption and decryption of data, usually in the form of files on (or sectors of) hard drives and removable media, email messages, or in the form of packets sent over computer networks. The school currently recommends the use of the Sophos Free Encryption tool for data encryption
Help Desk	Provides information and assistance to the users of the school's ICT systems
IAO	Information Asset Owner - see section 8.2
ICT	Information and Communications Technology.
ICT Systems	All computer and related systems within the school environment and also encompasses non computer based communication systems including TV, telephone etc.
Incremental backup	Backup in which only the data objects that have been modified since the time of some previous backup are copied.
MIS	Management Information System (SIMS)

network cabinet	Also know as a rack. A metal frame used to hold various hardware devices such as servers, hard disk drives, modems and other electronic equipment.
Network Manager	Person with overall responsibility for the school's admin and curriculum networks - Brian Harfoot
Portable and mobile devices	Any computing or communications device intended to frequently move location while maintaining function and operation, e.g. A mobile/smart phone, laptop computer etc.
SIRO	Senior Information Risk Officer - see section 8.1
Staff	A person employed by the school
UPS	A unit that switches to battery power whenever the mains power cuts out and allows time for ICT systems to be properly shut down or to continue to function until mains power is restored.
Users	Anyone that makes use of the ICT systems
Virus	A computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive.[2]Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer

Appendix 5: Mobile technology and e-safety when using mobile internet services

Developments in mobile technology have been rapid in recent years, meaning that mobile phones (and other personal devices) can now do much more than make voice calls. Integrated cameras, video messaging, mobile access to the internet, cloud-based services and location-based services are now commonplace, allowing access to a whole array of new content and services.

Children and young people have always been keen to grasp the opportunities offered by new technology and, with increasing rates of ownership at an ever lower age, mobile phones are no exception. However, as with any technology, there are associated risks: children and young people need to understand the issues, and develop appropriate strategies and behaviours, for keeping themselves safe.

This document focuses on the key e-safety considerations for personal use of mobile phones by children and young people, which should form part of their general e-safety education while in academy. There may be additional health and safety considerations if using mobile technologies in educational settings, and these are covered in a separate document.

As with e-safety issues generally, risks to young people can be broadly categorised under the headings of contact, content, culture and commerce. Key issues within each are outlined briefly below.

Contact

There is a risk that while online, a child or young person may make inappropriate 'friends', perhaps providing information or arranging a meeting that could risk his or her safety or the safety of others. This is perhaps the most worrying and extreme risk associated with fixed internet use.

With the mobile internet, these risks are potentially greater. Mobile phones are such personal and private devices, and so it will be difficult for parents to supervise access and contacts in the same way as they would a computer in the home. Mobile phones are typically always on and hence the owner is always contactable and, potentially, always vulnerable.

Additionally, location-tracking services may mean that it is possible to pinpoint the exact location of a mobile phone. While this may be welcomed by parents keen to know where their child is at all times, it is not difficult to see how the technology can be misused.

Content

As with the fixed internet, there is a risk that children and young people using mobile internet services may be exposed to material that is pornographic, hateful or violent in nature, or encourages activities that are dangerous or illegal. Equally so, content may simply be age inappropriate, inaccurate or misleading and, as outlined above, the scope for supervised access is obviously limited.

Network operators offer filtering and blocking services, typically switched on by default for pay-as-you-go accounts. Different settings may apply for pay monthly accounts where the registration process assumes that the user is 18 or over. Further information on available filtering options is available from the network operators direct (see below). Such services will not, however, filter inappropriate content sent directly to the user, such as text or picture messages.

Culture

The widespread use of mobile phones has brought with it a cultural shift.
Mobile phone users are typically always contactable which, although positive in many respects, can also mean that users never really 'switch off'. Late-night texting by teenagers, for example, may have a negative impact on sleep impairing concentration, academy work and general wellbeing.

Sexting is a growing concern. This is the act of sending sexually explicit messages or images to others using mobile phones and other online services. While often consensual in the first instance, young people often have no concept of the potential long-term impact of their actions. A key danger of sexting is the way in which material can quickly and easily be circulated or posted online, leaving the originator with no control over their images, often with embarrassing, and potentially devastating, consequences. Sexting is frequently linked to cases of bullying or harassment.

Mobile phones can also be used as a tool by bullies, using text messages as a tool to torment their victims. Camera phones can aggravate this further still, with many reported instances of people being photographed without their consent or knowledge, possibly in an inappropriate situation. This is an invasion of privacy, and can be extremely distressing for the subject of the photograph.

Acts of 'happy slapping' – an inappropriate term to describe a violent and disturbing form of bullying - have been well reported in the press. An assault is captured on a phone, then shared between phones or posted online, so adding to the misery and ridicule of the victim. This ease with which photographs or videos can be distributed is of particular concern. Once released in this way, it is impossible to permanently delete the images or files.

Additionally, photographs can inadvertently include clues as to an individuals' location, such as the academy name in the background, which if distributed inappropriately, could lead to the risk of contact by strangers. Mobile phones have also been used in cases of grooming, offering the offender easy access to their victim.

Other concerns include social networking or mobile blogging (the ability to update weblogs while on the move using mobile devices such as phones), with many young people posting content and images online of themselves and friends. A key concern is the level of personal information young people are making available, particularly with regard to their daily routines.

Additionally, the increasingly desirable nature of mobile phones means that young people owning them may become targets for theft.

Commerce

With the fixed internet there are concerns that a child could do something that has legal or financial consequences such as giving out a parent's credit card details or doing something that contravenes another persons' rights. Plagiarism and copyright are particular issues which are associated with the internet, especially in relation to downloading music or games. Research also shows that children are not able to differentiate between what is advertising and what is not.

Again, these present potential issues with the mobile internet with easy access to chargeable content and premium rate services in the form of games, downloads, ringtones, logos and other services all of which are particularly attractive to children and young people. Spam by text message

is also a problem, meaning that children and young people could be tricked into revealing personal information.

Helpful resources

- Premium rate services
    - PhonepayPlus (formerly ICSTIS) is the regulator of phone-paid services. They investigate complaints and give advice about premium rate services, scams and text services. Their Phonebrain website is designed to help children and young people stay in control of their money and troubleshoot premium rate problems.
- Mobile phone crime
    - The Out of Your Hands website focuses on mobile phone crime, and how we can help stop it. The website provides information and activities for young people (aged 7-16), teachers and youth leaders.
- Mobile operators
    - Mobile operators provide a range of information on the safe use of mobile phones:
        - O2
        - Orange
        - T-Mobile
        - Three
        - Virgin Mobile
        - Vodafone

Appendix 6: Mobile Device Policy 2017/18

written by Student Voice Mobile Technologies group, June 2012

Hall Cross Academy operates a philosophy of allowing students to develop their ability to use new technologies in an appropriate manner to enhance their learning. To this end, their mobile devices are permitted in school. Students should regard this as a privilege and treat this with the necessary respect. The following list of expectations were compiled by a group of students to outline students' responsibilities with their mobile device usage.

1. Mobile devices will be allowed to be brought to school.
2. Mobile devices are the responsibility of the owner of the device and the Academy is not liable for loss, theft or damage.
3. Mobile devices are not to be used during lesson times except with the express permission of the teacher for lesson and educational purposes.
4. Mobile devices are to only be used in lessons as an alternative to laptops, iPods or iPads which are provided by the Academy.
5. Mobile devices should not be charged using Academy electricity sockets or USB sockets on computers
6. Mobile devices can still be confiscated by staff if students disobey class instructions or use them without permission.
7. Mobile devices can be used outside of lessons along with access to the Academy wifi and network resources.
8. Students must access internet and other resources through the Academy wireless connection, rather than their own mobile internet provider, while in the Academy. Any attempt to circumvent the wifi filtering (eg. by using a VPN) will result in immediate loss of wifi access and possibly total network blocking.
9. Only appropriate websites as defined in the *e*safety policy and decided by staff can be accessed through wifi.
10. In accordance with the *e*safety policy, students must accept the trust placed in them by the Academy and agree to the responsible use of their mobile devices while on Academy premises. This includes not installing any apps or software that will enable their device to bypass school filtering and monitoring procedures.
11. Parents should be aware of students bringing their mobile devices into school
12. Unless express permission is granted mobile phones should not be used during lessons to make calls, send messages such as SMS, BBM or iMessage, surf the internet or take photographs or videos
13. When in lessons mobile devices should be on silent or turned off so as to not disturb the lesson with ringtones or alerts
14. Using a mobile phone to bully or threaten other students is not allowed and there will be severe consequences for students breaking this rule. Any incidents where a mobile device is used in connection with a bullying incident, illegal activity or malicious intent will result in removal of the privilege of being allowed the mobile phone in school and police involvement, where necessary
15. Mobile phones should not be taken into examination rooms in accordance with examination regulations
16. Teachers can, if they wish, allow students to use the functions on their mobile devices such as video or sound recording, cameras and internet access to aid in teaching and learning.
17. The privacy of mobile phone calls and texts is the responsibility of the students but other students or staff should not access the texts or calls of other students.
18. Students should not publish videos or photographs of other students or staff to social networks or distribute without their permission.

Appendix 7: Staff AUP

Academy Policy Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the school digital technology and communications systems, using Securus. This records all usage visible on a screen and reports can be generated if violations are recorded
- I understand that the Academy is taking action to reduce the risk of exposure to radicalisation / extremism online

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Academy.
- I understand that the network is the property of the academy and agree that my use must be compatible with my professional role.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only use academy communication systems for activity compatible with my professional role.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies. I will NOT have any students as "friends" on any personal social networking site and will report any incidents where students try to contact me through social networks.
- I will take all reasonable measures to ensure any personal social networking activity is subject to appropriate levels of security and will take the advice of IT Support where necessary.
- I recognise that any use of social networking that may compromise the integrity of Hall Cross Academy or any of its employees will be subject to disciplinary action

- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will not respond to emails from students' personal email accounts, if received. I will report any such emails to IT Support immediately.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems, unless it is in my non-teaching time.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to 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 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, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Personal Data Policy (or other relevant policy).

Where digital personal data is transferred outside the secure local network, it must be encrypted. An encrypted USB stick is provided by the academy for this purpose. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

The academy may exercise its right to monitor the use of the academy's information systems and internet access, to monitor email and to delete inappropriate materials where it believes unauthorised use of systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised, or unlawful, text, imagery or sound.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I understand that disciplinary action may be taken for any breach of these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 1: Use of mobile devices with the Academy

	Staff			Students			
	Allowed any time	Allowed only during non-teaching time	Not allowed	Allowed	Allowed only with staff permission	Allowed in non-lesson time	Not allowed
Mobile devices brought to school	✓			✓			
Mobile devices used in lessons as part of learning activity	✓				✓		
Taking photos / videos on mobile devices		✓			✓	✓	
Use of personal email address in school, or using school network		✓					✓
Use of school email system to send personal emails			✓				✓
Use of social media		✓				✓	
Use of blogs for personal reasons		✓				✓	
Sending a text message		✓				✓	
Making / taking a phone call		✓				✓	

Inappropriate Material, the Internet and E-mail

It is essential that teachers avoid situations both in and out with the classroom which could bring him/her into conflict with the Criminal Law or have an actual or perceived impact upon his/her standing as a teacher. Notwithstanding an individual's right to a private life, a teacher should, for example:

- not have in his/her possession at any time illegal materials/images in electronic or other format;
- not have in his/her possession inappropriate materials/images on academy premises;
- not download or access illegal images at anytime or in any place;
- not access inappropriate sites or download inappropriate materials on academy premises;
- ensure that he/she is fully aware of the academy's ICT guidelines and adhere to them;
- all communications with students/students must be justified in terms of learning and teaching.

In any event this should be carried out in a professional manner using an official academy email address and in strict compliance with academy ICT policies;

Professional Integrity

All staff/pupil relationships must be professional, appropriate and justifiable. Teachers should adhere to common sense and avoid inappropriate situations.

Teachers are entitled to a private life; however they must be conscious that they are role models for their students and that young people, in particular, may be strongly influenced by the conduct of teachers whether in or outside the classroom. Teachers should avoid inappropriate relationships with students and ensure that all communications are compatible with both their professional role.

Photographing/making videos of students must comply with the guidelines laid down by the Academy in the eSafety policy.

Blogging and Social Media Policy

Hall Cross Academy recognises the importance of the Internet and mobile communications technology in shaping public and internal thinking about the academy. We are committed to ensuring that all staff employed by the academy are aware of their vulnerability to identity theft and the potential threat to their profile and professional standing by posting inappropriate personal information on the internet via social networking sites thus leaving an "electronic footprint", compromising themselves and / or Hall Cross.

It's not just a matter of personal safety. What seems frivolous or even trivial to you in a friendship group could damage your reputation when seen by others. For example, pictures taken at parties and posted on a profile can cause embarrassment, or worse, when seen by parents, colleagues and employers. Before you post something, ask yourself what impression someone would get from seeing your web presence? Can this be linked back to my place of work and cause embarrassment or damage my professional role and /or Hall Cross?

This policy makes clear to all staff the steps necessary to protect themselves and the academy in making appropriate decisions about what content is suitable in blogs, personal & public websites, postings on wikis, video or picture sharing sites and when responding to comments from posts either publicly or via email. The Academy's ICT security policy and e-safety Policy remains in effect.

Please note that this policy applies only to online content that has a direct or indirect connection or link to Hall Cross or that may be inferred as being the opinion of Hall Cross. The policy does not infringe upon your personal interaction or commentary online unless the contents of such interaction or commentary are seen as a breach of professional trust between you and Hall Cross.

Interaction on the Internet and via mobile communication technology

- The Professional expectations of confidentiality regarding the day to day functions, practices and events that happen within Hall Cross do not change when using the internet or mobile communication technology. Staff are expected to speak respectfully about the academy and our current and potential employees, students, and partners. Do not engage in 'name calling'or behaviour that will reflect negatively on the academy's reputation. Note that the use of unfounded or derogatory statements or misrepresentation is not viewed favourably and may result in formal disciplinary action. Unless given permission by your line manager, you are not authorised to speak on behalf of the Academy, nor to represent that you do so
- Any online presence should not make reference to Hall Cross for example you are not authorised to utilise your academy email address when joining social networking sites for personal use or making the academy supplied email address your primary method of contact. There are separate guidelines in place for using the Academy email address when setting up a social networking account to be used explicitly for Academy communication
- The Hall Cross logo and name may not be used without explicit permission in writing from the Headteacher. This is to prevent the appearance that you speak for or represent the company officially
- Recognise that staff are legally liable for anything they write or present online. Staff may be formally disciplined by the academy for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. You may also become the subject of litigation by colleagues, and any individual or company that views your commentary, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment
- Honour the privacy rights of your colleagues by seeking their permission before writing about or displaying internal academy events that might be considered to be a breach of their privacy and confidentiality and ensure that the academy policy on displaying pupil images and information is adhered to
- Recognise that as a member of staff of Hall Cross Academy your online opinions, interactions and internet presence are influential to the young people that we support and as such should always be balanced and appropriate so that no inference of political, sexual or racist bias can be construed

The above points are not exhaustive and only cover a range of what the academy considers confidential and proprietary. If you have any questions about the appropriateness of online information released publicly or doubts of any kind, please speak to your line manager or a member of the senior leadership team before releasing information that could potentially harm our academy, or our staff, students, and academy community.

Appendix 9: Student AUP

Academy Policy Rationale

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the school / academy will monitor my use of the systems, devices and 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 understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line
- I understand that the Academy is taking action to reduce the risk of exposure to radicalisation / extremism online

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

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not try (unless I have permission) to 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 academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so

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, without the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission

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

- I will only use my own personal devices (mobile phones / USB devices etc) in school in line with the mobile device policy. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement and the Mobile Device Policy 2017/18, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings
- I will only use social media sites with permission and at the times that are allowed

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
- 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, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

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

- I understand that the academy 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 (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, fixed-term exclusions, contact with parents and in the event of illegal activities involvement of the police
- I will only use my school email account (@hallcrossacademy.co.uk) if I need to email a member of staff at the school
- I will not respond to emails sent to me by a member of staff's personal email address and I will report this if it happens
- I will not attempt to add any members of staff as friends on any social networking site
- I will not respond to any friend requests on any social networking sites from members of staff and I will report any such requests that are made

Please read the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. When you log onto a computer you will be asked to tick a box to confirm that you have read, understood and agree to the expectations. If you do not tick the box you will not be granted access to the Academy systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the academy systems and devices (both in and out of school)
- I use my own devices in the academy (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy eg communicating with other members of the school, accessing school email, VLE, website, on social media etc.

Policy developed in conjunction with SWGfL.