CASTLE HALL
ACADEMY

Online Safety Policy

Last Edited:	November 2018
Approval Date:	March 2017
Review Date:	November 2019

Table of Contents

1. Introduction
2. Responsibilities of the Academy community
3. Acceptable Use Policies (AUP)
4. Training
5. Learning and teaching
6. Parents and carers
7. Managing and safeguarding IT systems
8. Using the internet; email; publishing content online; using images, video & sound; using video conferencing and other online text or video meetings; using mobile phones; using other technologies
9. Protecting Academy data and information
10. Dealing with online safety incidents
11. Reference to related documents

Acknowledgement

This policy is based on an original document '**YHGfL Guidance for Creating an eSafety Policy'** written by Yorkshire and Humberside Grid for Learning. It has been adapted by Kirklees Learning Service for use in Kirklees schools. This policy has further been adapted for use at Castle Hall Academy.

Introduction

This Online Safety policy recognises the commitment of our Academy to keeping staff and students safe online and acknowledges its part in the Academy's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology. We believe the whole Academy community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with students.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and students to follow.

As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the Academy network and facilities from attack, compromise and inappropriate use and to protect Academy data and other information assets from loss or inappropriate use.

The scope of policy

- This policy applies to the whole Academy community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the Academy, visitors and all students.
- The Senior Leadership Team and Academy governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within the Academy will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety related incidents covered by this policy, which may take place outside the Academy, but is linked to membership of the Academy.
- The Education Act 2011 gives the Academy the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.
- The Academy will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of Academy.

This Online Safety policy was created by:

Mrs K Law, Head of Business and IT

David Firth Senior IT Technician at Castle Hall Academy.

The following groups were consulted during the creation of this Online Safety policy:

The policy was completed on:

28th November 2018

Implementation of the policy

- The Senior Leadership Team will ensure all members of the Academy staff are aware of the contents of the Academy Online Safety Policy and the use of any new technology within the Academy.
- All staff, students, occasional and external users of our Academy IT equipment will sign the relevant Acceptable Use Policies
- All amendments will be published and awareness sessions will be held for all members of the Academy community.
- Online safety will be taught as part of the curriculum in an age-appropriate way to all students.
- Online safety posters will be prominently displayed around the Academy.
- The Online Safety Policy will be made available to parents, carers and others via the Academy website or VLE.

The following local and national guidance are acknowledged and included as part of our Online Safety Policy:

1. **Kirklees LSCB Guidance**

The Kirklees Safeguarding Children's Board Procedures and Guidance

Kirklees Safeguarding procedures will be followed where an online safety issue occurs which gives rise to any concerns related to child protection. In particular we acknowledge the specific guidance in:

Section 1.4.6 Child Abuse and Information Communication Technology

This section of the Kirklees Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the internet. In particular we note and will follow the advice given in the following section:

Section 7 Actions to be taken where an Employee has Concerns about a Colleague

This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

2. Government Guidance

Keeping Children Safe in Education (DfE 2018) with particular reference to Annex C Online Safety

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2015)

How social media is used to encourage travel to Syria and Iraq - Briefing note for schools (DfE 2015)

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014) Advice on Child Internet Safety 1.0

Universal Guidelines for Providers (DfE and UKSIC 2012)

3. Kirklees Guidance

The following Kirklees Guidance documents are included as part of this Online Safety Policy:

Kirklees Electronic Communications Guidance for Academy Staff

Kirklees First Responders Guidance for Academy Staff

The following document is included for information

Misuse of Electronic Communications – information for all Kirklees staff

Responsibilities of the Academy Community

We believe that online safety is the responsibility of the whole Academy community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Senior Leadership Team accepts the following responsibilities:

- The Headteacher and Designated Safeguarding Lead will take ultimate responsibility for the online safety of the Academy community
- Identify a person Mrs K Law, Head of Vocational Skills to take day to day responsibility for online safety; provide them with training; monitor and support them in their work
- Ensure adequate technical support is in place to maintain a secure IT system
- Ensure policies and procedures are in place to ensure the integrity of the Academy's information and data assets
- Ensure liaison with the governors
- Develop and promote an online safety culture within the Academy community
- Ensure that all staff, students and other users agree to the Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the Academy community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur inside the Academy and review incidents to see if further action is required

Responsibilities of the Online Safety Lead

- Promote an awareness and commitment to online safety throughout the Academy
- Be the first point of contact in the Academy on all online safety matters
- Take day to day responsibility for online safety within the Academy
- Lead the Academy online safety team and/or liaise with technical staff on online safety issues
- Create and maintain online safety policies and procedures
- Develop an understanding of current online safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in online safety issues
- Ensure that online safety education is embedded across the curriculum
- Ensure that online safety is promoted to parents and carers
- Ensure that any person who is not a member of the Academy staff, who makes use of the Academy IT equipment in any context, is made aware of the Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on online safety issues to the online safety group, the Senior Leadership Team and the Safeguarding/Online Safety Governor as appropriate
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- Ensure an online safety incident log is kept up to date
- Ensure that Good Practice Guides for online safety are displayed in classrooms and around the Academy
- To promote the positive use of modern technologies and the internet
- To ensure that the Academy Online Safety Policy and Acceptable Use Policies are reviewed at prearranged time intervals.

Responsibilities of all Staff

- Read, understand and help promote the Academy's online safety policies and guidance
- Read, understand and adhere to the Staff IT AUP.
- Take responsibility for ensuring the safety of sensitive Academy data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with students is on a professional level and only through Academy based systems, **NEVER** through personal email, text, mobile phone social network or other online medium.

- Embed online safety messages in learning activities where appropriate
- Supervise students carefully when engaged in learning activities involving technology
- Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log (currently CPOMS).
- Respect, and share with students the feelings, rights, values and intellectual property of others in their use of technology in Academy and at home

Additional Responsibilities of Technical Staff

- Support the Academy in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the Academy IT systems, sensitive data and information. Review these regularly to ensure they are up to date

- Ensure that provision exists for misuse detection and malicious attack

- At the request of the Senior Leadership Team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any online safety related issues that come to their attention to the Online Safety Lead and/or Senior Leadership Team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the Academy's IT equipment
- Liaise with the Local Authority and others on online safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- This links to the Network Infrastructure Policy November 2017.

Responsibilities of Students

- Read, understand and adhere to the Student AUP and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of the Academy
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in Academy and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow Academy policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow Academy policies regarding online bullying

Responsibilities of Parents and Carers

- Help and support the Academy in promoting online safety
- Read, understand and promote the Student AUP with their children
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the Academy if they have any concerns about their child's use of technology
- To agree to and sign the Home Academy Agreement within the student planner containing a statement regarding their personal use of social networks in relation to the Academy:

Responsibilities of the Governing Body

- Read, understand, contribute to and help promote the Academy's online safety policies and guidance as part of the Academy's overarching safeguarding procedures
- Support the work of the Academy in promoting and ensuring safe and responsible use of technology in and out of the Academy, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the Academy IT infrastructure provides safe access to the internet and the steps the Academy takes to protect personal and sensitive data

Ensure appropriate funding and resources are available for the Academy to implement their online safety strategy

Responsibilities of the Designated Safeguarding Lead

- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, online bullying, radicalisation and others.
- Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media and relevant websites/newsletters.
- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.
- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to online safety ensuring that staff know the correct child protection procedures to follow.

Responsibility of any external users of the Academy systems e.g. adult or community education groups; breakfast or after-school club

- Take responsibility for liaising with the Academy on appropriate use of the Academy's IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants follow agreed Acceptable Use Procedures
- They will be emailed in advance the policies to be signed and returned

Acceptable Use Policies

Castle Hall Academy has a number of AUPs for different groups of users.
These are shared with all users yearly and staff and students will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to Academy who use our IT facilities are made aware of the appropriate AUP.

Academy Acceptable Use Policy documents

Staff Acceptable Usage Policy [version 2018]
Student Acceptable Usage Policy [version 2018]
Visitors and Supply Teachers Acceptable Usage Policy [version 2018]
Home Academy Agreement Policy [version 2018]
Mobile Technologies Acceptable Usage Policy 2017
Social Media Acceptable Usage Policy 2018
Use of Digital and Video Images Acceptable Usage Policy 2017
Sanctions for Improper use of IT facilities Policy [version 2017] (students only)
Academy Network Infrastructure Policy 2017
Academy Data Backup and Disaster Recovery Policy 2017

Versions of these documents are included in the references at the end of the policy

Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. The Online Safety Lead will attend training updates at least once per year. All Academy staff will receive regular updates on risks to students online from the Online Safety Lead, and attend online or external training as necessary.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our Academy community lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just inside the Academy but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that students have a growing understanding of how to manage the risks involved in online activity. We believe that learning about online safety should be embedded across the curriculum and also taught in specific lessons such as in Computing and PSCHE.

We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and students will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind students about the responsibilities to which they have agreed through the AUP.

Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Schemes of work available on request.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the Academy newsletter and website.

We will ask all parents to discuss the student AUP with their child and sign the Home Academy Agreement in their planners. We ask parents to sign the Home Academy Agreement which includes a statement about their use of social networks in situations where it could reflect on our Academy's reputation and on individuals within the Academy community.

We request our parents to support the Academy in applying the Online Safety Policy.

Managing and safeguarding IT systems

The Academy will ensure that access to the Academy IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for Academy activity.

All administrator or master passwords for Academy IT systems are kept secure and available to at least two members of staff e.g. the Headteacher and Network Manager, Senior Technician on site.

The wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access by named individuals e.g. a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are not allowed administrator rights to download software on Academy provided laptops.

Filtering Internet access

Web filtering of internet content is currently provided by ICT4C. The Academy also has a second internet connection used only by teaching staff and is filtered and secured by SmoothWall. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in students in monitoring their own internet activity.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

Monitoring

In order to be compliant with the Prevent Duty and Keeping Children safe in Education 2018, the school will:

- Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.

- The ICT Office has a program called ABTUTOR which we use to support any staff who are experiencing technical issues, but the software can is also used to monitor students suspected of breaking the rules of using ICT equipment. Using ABTUTOR we can easily evidence misuse of school technology and deal with the culprits as necessary by collecting screenshots and screen recordings. ABTUTOR is also installed in 3 ICT rooms for teachers to monitor the student PC's in each of those rooms. This allows teaching staff to also monitor, control and restricts student's activity within the ICT rooms.

- All student usage of the schools email (communication) system is recorded and stored within the cloud. Members of the schools technical and online safety team have access to these records and the communication between students is checked on a regular basis.

Access to Academy systems

The Academy decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the Academy who may be granted a temporary log in.

All users are provided with a log in appropriate to their role in the Academy.

Students are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and Academy and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to Academy systems is covered by specific agreements and is never allowed to unauthorised third party users.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, Academy management information system).
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within Academy.
- All staff are prompted to changed their passwords every each term.
- All students have a unique, individually-named user account and password for access to IT equipment and information systems available within Academy.
- All staff and students have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security to the IT Network Manager.
  The Academy maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the Academy's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the Academy IT systems or an Academy provided laptop or device and that such activity can be monitored and checked.

All users of the Academy IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Students and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around Academy.

Using email

Email is regarded as an essential means of communication and the Academy provides all members of the Academy community with an e-mail account for Academy based communication. Communication by email

between staff, students and parents will only be made using the Academy email account and should be professional and related to Academy matters only. Email messages on Academy business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the Academy is maintained. There are systems in place for storing relevant electronic communications which take place between the Academy and parents.

Use of the Academy email system is monitored and checked.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum students are taught about safe and appropriate use of email. Students are informed that misuse of email will result in a loss of privileges.

The Academy will educate students on appropriate communication with staff/others.

Under no circumstances will staff contact students, parents or conduct any Academy business using a personal email addresses.

Responsible use of personal web mail accounts on Academy systems is permitted during freetime.

Publishing content online

E.g. using the Academy website, Learning Platform, blogs, wikis, podcasts, social network sites

Academy website:

The Academy maintains editorial responsibility for any Academy initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The Academy maintains the integrity of the Academy web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the Academy address, e-mail and telephone number. Contact details for staff published are Academy provided.

Identities of students are protected at all times. The Academy obtains permission from parents for the use of students' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:

As part of the curriculum we encourage students to create online content. Students are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the Academy where possible. Students will only be allowed to post or create content on sites where members of the public have access when this is part of an Academy related activity. Appropriate procedures to protect the identity of students will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the Academy:

Staff and students are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside the Academy as they are within the Academy.

Material published by students, governors and staff in a social context which is considered to bring the Academy into disrepute or considered harmful to, or harassment of another student or member of the Academy community will be considered a breach of Academy discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Students are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of students wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of students' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and on the website.

For their own protection staff or other visitors to the Academy never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of students.

We are happy for parents to take photographs at Academy events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

Using video conferencing, web cameras and other online meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. We ensure that staff and students take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Students do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and student(s) which takes place outside the Academy or whilst the member of staff is alone is always conducted with the prior knowledge of the Headteacher or line manager and respective parents and carers.

Using mobile phones

Use of mobile phones by students is covered by a separate policy.

During lesson time we expect all mobile phones belonging to staff to be switched off unless there is a specific agreement for this not to be the case.

Where required for safety reasons in off-site activities, an Academy mobile phone is provided for staff for contact with students, parents or the Academy. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a student or parent. (*In an emergency, where a staff member doesn't have access to a Academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.)*

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material which causes distress to the person(s) concerned will be considered a breach of Academy discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another student or staff member we do not consider it a defense that the activity took place outside Academy hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

We make it clear to staff, students and parents that the Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for students. However their use in lesson time will only be with permission from the teacher and within clearly defined boundaries.

Students are taught to use them responsibly.

Using wearable technology

The use of wearable technology includes electronic fitness trackers and internet enabled 'smart' watches for students is covered by separate guidance (Student Mobile Phone Policy).

Wearable technology by staff is permitted on school premises, but must not be used during lessons, unless it adds value to the teaching and learning of students.

Personal devices are brought onto school premises by pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

Wearable technology is not to be worn during tests or examinations.

Using other technologies

As an Academy we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by students.

Staff using a technology not specifically mentioned in this policy, or a personal device, whether connected to the Academy network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document and Staff IT AUP.

Students are not to use own devices within the academy without special permission from the Headteacher and IT network manager/Senior Technician.

Protecting Academy data and information

The Academy recognises their obligation to safeguard staff and students' sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The Academy is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the Academy will be controlled appropriately through technical and non-technical access controls.

Students are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties. This is taught through e-safety lessons in Key Stage 3 Computing and through PHSCE curriculum.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with a means of encrypting USB memory sticks for carrying sensitive data
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the Academy management information system holding student data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside the Academy. [See Staff AUP and DPSP policy]
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them. [See DPSP].
- We follow Kirklees procedures for transmitting data securely and sensitive data is not sent via email unless encrypted
- Remote access to computers is by authorised personnel only and via secure gateway
- We have full back up and recovery procedures in place for Academy data. [See Academy Data Backup and Disaster Recovery Policy].
- Where sensitive staff or student data is shared with other people who have a right to see the information, for example governors, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.

Management of assets

Details of all Academy-owned hardware and software are recorded in an inventory.

All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any IT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Dealing with online safety incidents

All online safety incidents are recorded on the Academy CPOMS system which is regularly reviewed.

Any incidents where students do not follow the Acceptable Use Policy will be dealt with following the Academy's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning students or staff, they will inform the Designated Safeguarding Lead, their line manager or the Headteacher who will then respond in the most appropriate manner. The member of staff must also record the incident/concern on CPOMS.

Instances of **online bullying** will be taken very seriously by the Academy and dealt with using the Academy's anti-bullying procedures. The Academy recognises that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the Academy network, or create an information security risk, will be referred to the Academy's Online Safety Lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any

policies, procedures or guidance. If the action breaches Academy policy then appropriate sanctions will be applied. The Academy will decide if parents need to be informed if there is a risk that student data has been lost.

The Academy reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:
If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then the procedures outlined in Castle Hall Academy Child Protection Policy and Castle Hall Academy Safeguarding Policy should be followed. All incidents should be logged on CPOMS and the DSL made aware.

Dealing with complaints and breaches of conduct by students:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff / DSL or if appropriate the Headteacher.
- Parents and the student will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment or of a bullying nature after being warned
- staff using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)
- Using technology to promote/support, participate in or encourage any form of radicalisation and extremism.

The following activities are likely to result in disciplinary action:

- any online activity by a member of the Academy community which is likely to adversely impact on the reputation of the Academy
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at Academy or in lessons sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using Academy or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the Academy into disrepute
- attempting to circumvent Academy filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing Academy IT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Guidance for staff on the consequences of the misuse of electronic equipment can be found in the document **'Staff Code of Conduct'**

References to related documents:

- Acceptable Use Policies (Students, Staff, Visitors and Supply staff)
- Letter for Parents explaining the AUP and Home Academy Agreement to sign
- IT Sanctions policy linked to Academy BFL
- Data Protection and security policy (DPSP)
- Email policy [See Student AUP, Staff AUP and Visitor and Supply Teachers AUP)
- Academy Data Backup and Disaster Recovery Policy
- First responds guide to Online Safety Incidents
- Castle Hall Academy Child Protection Policy