The Bulwell Academy

E-Safety Policy

Issued: July 2017

To be reviewed annually

Bulwell Academy

Supported by the Edge Foundation

Introduction

The Bulwell Academy recognises the benefits and opportunities that new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

However, the use of these new technologies can put young people at risk, both within and outside the academy. Some of the dangers our students may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, the loss of, or the sharing of personal information
- The risk of grooming by those with whom they make contact on the internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others including strangers
- Cyber-bullying (See Appendix 1)
- Access to unsuitable video or internet games
- An inability to evaluate the quality, accuracy, appropriateness and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use of technology which may impact on the social and emotional development and on the learning of the young person.

Our approach is to implement appropriate safeguards within the academy whilst supporting staff and learners to identify and manage risks independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This E-Safety policy should be read alongside other relevant Academy policies/guidance:

- Safeguarding/Child Protection Policy
- IT Acceptable Use Policy Staff and Student
- Anti-Bullying Policy
- Mobile Telephone Policy
- Behaviour Policy
- Equal Opportunities

Monitoring and Review

The impact of the policy will be monitored regularly with a full review being carried out yearly or more frequently, dependent on particular national issues or internal issues that may be raised which impact on our use of e safety.

The implementation of this E-Safety policy will be monitored by:	• IT Systems Manager • Safeguarding – The Principal & the Attendance & Safeguarding Manager • E-Safety Coordinator (ICT Head of Department)
The Governing Body will receive updates of the implementation of E-Safety at regular intervals: half-yearly	Half yearly
The E-Safety policy will be reviewed annually, or more frequently in the light of any significant developments in the use of technologies, new threats to E-Safety or incidents that have taken place.	June 2018
Should serious E-Safety incidents take place, the following persons should be informed:	• E-Safety Coordinator • IT Systems Manager • Safeguarding

The Academy will monitor the impact of the policy using:

- Logs of reported incidents (supported by Year VPs)
- Monitoring logs of Internet Activity including sites visited
- Internal monitoring of network activity
- Surveys/questionnaires of:
    - Students
    - Parents/carers
    - Staff

Policy

The policy applies to all users/all students and staff/all members of the Bulwell Academy community who have access to the academy's IT systems, both on the premises and remotely.

Any user of School IT systems must adhere to the E-Safety Rules and the Acceptable Use Agreement.

The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

The Academy will deal with any unacceptable behaviour outlined within this policy and associated behaviour and anti-bullying policies and will, where known and deemed appropriate, inform parents/carers of incidents of inappropriate E-Safety behaviours that occur in and out of the Academy.

Roles and Responsibility

Concern:	**Report to:**
Safeguarding	Attendance & Safeguarding Manager
IT or equipment	IT Systems Manager
E-Safety	E-Safety Coordinator

The school will monitor the impact of the policy using:

- Regular questioning or surveying of
    - Students
    - Parents and Guardians
    - Staff
- Logs of reported incidents
- Internal monitoring data for network activity

Principal

- The Principal is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to an E-Safety Coordinator.
- The Principal and Senior Vice Principal are responsible for ensuring the E-Safety Coordinator and other key staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team (SLT) will receive regular monitoring reports from the E-Safety Coordinator.
- The Principal and Senior Vice Principal should be aware of all procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

E-Safety Coordinator

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the Academy E-Safety policies and documents.
- Meets regularly with the Vice Principal for ICT and provides regular reports to other members of the Senior Management Team.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Academy's ICT technical staff to ensure that the ICT infrastructure is secure and is not open to misuse or malicious attack.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Ensures that they keep themselves up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- Liaise with the ICT Manager to ensure that the use of the network including remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported.
- Liaise with the ICT Manager to ensure that monitoring software and systems are implemented and updated as agreed in Academy policies.

IT Systems Manager/Technical Staff

- Ensures that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack. Also that the Academy meets required E-Safety technical requirements and any Local Authority E-Safety policy/guidance which may apply
- Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Ensures that the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Ensures that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- To Ensure that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety committee
- That there are monitoring software/systems implemented and that they are kept up-to-date

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current Academy e- Safety policy and practices.
- They have read, understood and signed the Academy ICT Staff Code of Conduct.
- They report any suspected misuse or problem to the E-Safety Co-ordinator.
- Digital communications with Students are on a professional level only.
- E-Safety issues are embedded in all aspects of the curriculum and other academy activities.
- Students understand and follow the Academy E-Safety and student Acceptable Use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended Academy activities.
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices.

Safeguarding Officers

Should be trained in E-Safety issues and be aware of the potential for serious child protection issues which may arise from:

- Sharing of personal data.
- Access to illegal or inappropriate materials.
- Inappropriate on-line contact with adults or strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

E-Safety Committee

The E-Safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety policy including the impact of initiatives. The group will be responsible for regular reporting to the Governing Body. All members of the committee will assist the E-Safety Coordinator with:

- The production/review/monitoring of the Academy E-Safety policy/documents
- The production/review/monitoring of the Academy filtering policy and requests for filtering changes
- Mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/incident logs (with support from Year VPs and Year Managers)
- Consulting stakeholders – including parents/carers and the students about the E-Safety provision
- Monitoring improvement

Students

- Are responsible for using the academy's ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to Academy systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand academy guidance on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy policies on the taking and use of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies off site and realise that the Academy's E-Safety Policy covers their actions out of academy, if related to their membership of the academy.
- Students will be required to accept the 'acceptable use' terms and conditions when they log onto the Academy network

Parents/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The Academy will therefore take the opportunity to help parents understand these issues through parents' evenings, letters, and other literature. Once a year there will also be an information event where parents will receive a briefing on potential E-Safety matters, have the opportunity to meet the E-Safety committee and be able to seek advice and guidance to support their child's safe use of the Internet

Parents and guardians will be responsible for endorsing (by signature) the Student Acceptable Use Policy.

Parents will also be kept up-to-date through the publishing of material on the Academy website and via parental mail out and emails, and through the delivery of Parent Information Evenings.

Security

The Bulwell Academy will do all that it can to make sure the network is safe and secure. Every effort is made to keep security software up to date. Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc.

The Bulwell Academy reserves the right to monitor all internet activity undertaken by staff and students.

Multiple levels of safeguarding and E-Safety.

'Smoothwall' is a filtering system which keeps lists of sites and categories of sites which are not to be permitted and blocks staff/students from accessing these sites. We are able to add/remove sites to these lists if new threats emerge. The appliance also logs attempts to access suspect sites which we can use to generate reports.

We also use a product called Impero which allows staff to actively monitor students' use of the PCs. It also keeps a log of everything the student does on any PC. In addition, Impero flags suspicious/worrying activity. The system also automatically takes a screenshot of the activity. Staff use Impero around the Academy to monitor their areas. This tool allows them greater control over PC use and highlights areas of concern/misuse very early.

Email is also monitored by our email appliance. As well as junk filtering the appliance monitors student email and automatically flags concerning phrases/words to the IT Team.

Risk Assessment

Risk assessment procedures are in place whenever new technologies are being considered by the IT team. All software is installed through the IT Team. This includes the use of DVDs.

Behaviour

The Bulwell Academy will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy and related policies.

The Bulwell Academy will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable, the Academy will deal with the matter internally. Where conduct is considered illegal, the Academy will report the matter to the police.

Communications

The Bulwell Academy requires all users of IT to adhere to the strict rule which states clearly all student mobile phones must be switched off during the Academy day.

Personal Information

Any processing of personal information needs to be in compliance with the Data Protection Act 1998. Any device on which images are stored must be immediately given to the IT Team for approval and storage. Images must not be shared by staff or students.

The Bulwell Academy collects and stores the personal information of students and staff. The Academy will keep that information safe and secure and will not pass it on to anyone else without the express permission of the learner/parent/ carer.

No staff/students' personal information will be available on the website.

Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information is password protected. No personal information of individuals is permitted offsite. Every user of IT facilities is required to log off on completion of any activity, or when they are physically absent from a device for any period this continues at regular intervals throughout the student's time at the Academy.

All Academy mobile devices such as a laptop should be password protected, and this should be changed periodically. Staff should ensure that the information held on the laptop is kept safe and no unauthorised access takes place.

Use of image and video

No image/photographs of students or student based activities should be copied, downloaded, shared or distributed online. Photographs of activities on the Academy premises should be considered carefully and have the right consent prior to any usage. Students are not permitted to take any pictures on academy site unless related to an educational reason and only when full consent is granted. Approved photographs should not include names of individuals without consent.

Education and Training

With the current unlimited nature of internet access, it is impossible for the Bulwell Academy to eliminate all risks for staff and learners. It is our view, therefore, that the academy should support staff and learners to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

Students

E-Safety will be covered in the following ways:

- All Year 7: Multimedia Unit focusing on E-Safety (ICT Department)
- All Year 8: Animation Unit focusing on E-Safety (ICT Department)
- Years 7-11: PSHE programme (Whole Academy)

Key E-Safety messages will be reinforced as part of a planned key facts distribution by the E-Safety Coordinator.

Students should be taught in other curriculum areas to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Students should be helped to understand the need for the student Acceptable Usage Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the academy.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Staff

Staff should act as good role models in their use of ICT, the internet and mobile devices.

In lessons where internet use is pre-planned, it is best practice that Students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Websites can be blocked and unblocked with reference to the IT Manager.

Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- Formal E-Safety training will be made available to staff. An audit of the E-Safety training needs of all staff will be carried out regularly.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the academy E-Safety policy and Acceptable Use Policies.
- The E-Safety Coordinator will receive regular updates through attendance at training sessions and by reviewing any guidance documents released.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff INSET days.
- The E-Safety Coordinator will provide advice, guidance and training to individuals as required.

Incidents and Response

Where an E-Safety incident is reported to the Academy, the matter will be dealt with very seriously. The Academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a student wishes to report an incident, they can do so to their Teaching and Learning Leader or Vice Principal, Personal Tutor or other appropriate staff member. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible or designated E-Safety Coordinator.

Following any incident, the Academy will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

All incidents will be recorded on a centralised system so incidents can be logged, monitored and reviewed regularly to see if additional changes are needed to be made.

Feedback and Further Information

Bulwell Academy welcomes all constructive feedback on this and any other Academy policy. If you would like further information then please contact our E-Safety Coordinator.

Appendices

- Cyberbullying
- Acceptable Usage Policy (Student and Staff Agreements)
- Academy Actions and Sanctions reference Table

Appendix 1: Cyberbullying

Cyberbullying is defined in legal glossaries as

- actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
- use of communication technologies for the intention of harming another person
- use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

Cyberbullying is emerging as one of the more challenging issues facing educators and parents as young people embrace the Internet and other mobile communication technologies.

Cyber threats are a related concern. A cyber threat is online material that threatens or raises concerns about violence against others, suicide, or other self-harm.

We know from research that mobile bullying is a widespread problem for young people across the UK. Teachers are concerned their students could be bullied by mobile phones. It is important parents and teachers have a common understanding of this issue and work together to prevent cyberbullying.

Making anonymous or abusive phone calls, sending a malicious or threatening text message or email is a criminal offence.

Cyberbullying can include:

- **Text message bullying** – sending unwelcome texts that are threatening or cause discomfort.
- **Picture/video-clip bullying via mobile phone cameras** – used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. For example, so-called 'Happy slapping' involves filming and sharing physical attacks.
- **Phone call bullying via mobile phone** - silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- **Email bullying** – uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Chat room bullying** - involves sending menacing or upsetting responses to children or young people when they are in a web based chat room.
- **Bullying through instant messaging (IM)** - an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites -** includes the use of defamatory blogs (weblogs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

The Academy has a duty to ensure that:

- Bullying via mobile phone or the Internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with cyberbullying in the Academy.
- The curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely.
- All e-communications used on the academy site or as part of Academy activities off-site are monitored.
- Clear policies are set about the use of mobile phones at the Academy and at other times when young people are under the Academy's authority.
- Internet blocking technologies are continually updated and harmful sites blocked.
- They work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice.
- Security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside the Academy.
- They work with the police and other partners on managing cyberbullying.

Appendix 2a: Acceptable Usage Policy – ICT (Student Agreement)

The Academy has provided computers for use by students, offering access to a vast amount of information for use in studies, acting like an enormous extension to the Academy library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the internet just as you are in a classroom or in an Academy corridor. Remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

The Academy provides a screening service for internet use. However no solution can completely guarantee the prevention of students' access to unwanted internet material. Articles of unacceptable material such as racist, extremist, political or violent material for example, are not as easy to screen out as pornography; however we work closely with our internet provider to ensure such sites are filtered. Computers will be used to access the internet only where staff can monitor their use.

Equipment

- Installing, attempting to install or storing programs of any type on the computers is not allowed. If you need a specific program for your studies you will need to talk to the Network Manager or your teacher.
- Damaging, disabling or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Flash Games are not permitted in the Academy, unless authorised by a member of staff supervising the lesson.
- Always check files brought in on a removable media (such as CDs, flash, drives etc.) with antivirus software and only use them when they are found to be clean of viruses.
- Mobile equipment (e.g. laptops, tablet PC's, PDAs etc.) are not allowed to be connected to the network unless an additional agreement has been signed following a meeting with the network manager.
- No eating or drinking is allowed in the IT rooms to protect the computers from spillages.
- Do not use the network in any way that would disrupt use of the network by others.
- Unapproved system utilities and executable files will not be allowed in work areas, attached to email or run from an external drive.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name and password.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas and portable storage will be treated as Academy books. Staff may review your files and communications at any time to ensure that you are using the system responsibly.
- Do not reveal and personal information e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- The Academy has trained internet safety advisers. If you are concerned about any issues regarding the use of the internet or contact you have had via the internet please talk to your tutor who will be able to refer you to an adviser.

Internet

- Access to the internet at Academy and use of the Academy network are privileges not rights.
- You should access the internet only for study or for Academy authorised/supervised activities.
- Only access suitable material – using the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted. You are responsible for rejecting these links if any appear inadvertently during your research.
- Respect the work and ownership rights of people outside the Academy, as well as other students and staff. This includes abiding by copyright and intellectual property rights.

- Do not try and bypass the filters which are in place as they are there for your protection. If you find unsuitable websites through the use of proxy servers you should report the web address to the network manager.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the internet as on the street. You should remember that you are representatives of the Academy on a global public system.
- Only open attachments to emails if they come from someone you already know and trust. Attachments contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The Academy will treat this misuse in line with the Academy's code of conduct.
- The sending or receiving of an email containing content likely to be unsuitable for children or educational organisations is strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Electronic mail – is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.

Please read this document carefully. Only once it has been signed and returned will access to the internet be permitted. If you violate these provisions, access to the internet will lead to removal of all ICT access.

Additional action may be taken by the Academy in line with existing policy regarding Academy behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, Police may be involved or other legal action taken.

I have read and understand the above and agree to use the Academy computer facilities within these guidelines.

Student Name: _____ Tutor Group: _____

Student Signature: _____

I have read and understood the above.

Parent/Guardian Signature: _____ Date: _____

A copy of this form can be found on the Academy's website.

Appendix 2a: Acceptable Usage Policy – ICT (Staff Agreement)

The aim of this policy is to provide clarification to staff on the use of emerging technologies so that a teacher's professional position is not compromised. It should be read in conjunction with the Child Protection Policy which offers further guidance on safeguarding issues.

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

For my professional and personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of the Academy ICT systems (e.g. laptops, email, etc) out of the Academy, and to the transfer of personal data (digital or paper based) out of the Academy
- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use
- 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 not communicate with students through social networking sites such as Facebook or on Twitter. I will not under any circumstances accept friend requests from a person who I believe to be either a parent/carer or a student at the Academy. I am responsible for ensuring that privacy settings are enabled and that private content is not available to students. If I require support with this the IT staff will help me
- I will not issue my mobile phone number to students or ask for students' mobile phone numbers or keep a record of student mobile phone numbers for reasons other than official Academy business e.g. speaking to parents
- 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 ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Academy'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.
- I will not use chat and social networking sites in the Academy in accordance with the Academy Policy
- I will only communicate with students and parents/carers using official Academy systems. Any such communication will be professional in tone and manner and any protracted communication will be referred to my line manager
- 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 (PDAs/laptops/mobile phones/USB devices etc) in the Academy, 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
- 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 programs)
- 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 programs 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 programs of any type on a machine, or store programs 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. Where digital personal data is transferred outside the secure local network, it must be encrypted. 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 Academy 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 ICT equipment in the Academy, but also applies to my use of Academy ICT 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.

I have read and understand the above and agree to use the Academy's ICT systems (both in and out of the Academy) and my own devices (in the Academy and when carrying out communications related to the Academy) within these guidelines.

Staff Name (Print)

Signed

Date

Actions and Sanctions

The Academy believes that the activities referred to in the following section would be unacceptable in an Academy context and that users should not engage in these activities in Academy or when using Academy equipment or systems.

		Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images		√
	Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation		√
	Adult material that potentially breaches the Obscene Publications Act in the UK		√
	Criminally racist material in UK		√
	Pornography	√	
	Promotion of any kind of discrimination	√	
	Promotion of racial or religious hatred	√	
	Threatening behaviour, including promotion of physical violence or mental harm	√	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the Academy into disrepute	√	
Using Academy systems to run a private business		√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy		√	
Uploading downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		√	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)		√	
Creating or propagating computer viruses or other harmful files		√	

Actions and sanctions for incidents involving Students relating to the use of the Academy system. The response would depend on the severity and frequency of the incident.

Incidents	Warning	Refer to technical staff for action e.g. filtering/security etc.	Refer to Year team	Removal of network/internet access rights	Refer to Principal	Inform parents of Guardians	Further sanction e.g. detention or exclusion	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see above for list on unsuitable and inappropriate activities).					√	√	√	√
Unauthorised use of non-educational sites during lessons	√	√	√					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√	√	√					
Unauthorised use of social networking, instant messaging, personal email	√	√	√					
Unauthorised downloading or uploading of files		√	√	√				
Allowing others to access Academy network by sharing username and passwords			√	√				
Attempting to access or accessing the Academy network, using another Student's account			√	√				
Attempting to access or accessing the Academy network, using the account of a member of staff			√	√	√	√		
Corrupting or destroying the data of other users				√	√	√		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			√	√	√	√		
Continued infringements of the above, following previous warnings or sanctions							√	
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy					√	√	√	
Using proxy sites or other means to subvert the Academy's filtering system			√	√	√	√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident			√	√	√	√	√	
Deliberately accessing or trying to access offensive or pornographic material					√	√	√	
Deliberately attempting to access protected areas of the network (Hacking)					√	√	√	