TRINITY ACADEMY NEWCASTLE TRUST

E-Safety and Acceptable Use Policy

Approved by the Committee – October 2017
On behalf of the Board
Next Review Date – October 2018

E-safety and Acceptable Use of ICT Policy

This E-safety and Acceptable Use of ICT Policy (AUP) relates to all members of the Trinity Academy community (including learners, staff, volunteers, visitors and contractors) who have access to, and are users of ICT systems and resources both in and out of learning venues where actions relate to Academy set activities or use of Academy online systems.

Context

To prepare learners for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and learners into contact with a wide variety influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the Academy environment. Current and emerging technologies in Academy and more importantly, in many cases outside the Academy by learners include:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- PDA’s
- Smart phones with e-mail and web applications

All of these have potential to help raise standards of teaching and learning, but may equally present challenges to both learners and tutors in terms of keeping themselves safe. These challenges include:

- Exposure to inappropriate material
- Exposure to Extremism and Radicalisation
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising online gambling and financial scams
- Safeguarding issues such as Sexual Exploitation (Children or vulnerable adults)
- Other illegal activities

At Trinity Academy we seek to maximise the educational benefit that can be obtained by exploiting the use of ICT, whilst at the same time minimising any associated risks. By making clear to learners, staff, volunteers, contractors etc. what the Academy expectations

are regarding the use of ICT, we aim to protect our learners and staff from harm, as far as reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads and fashions change but there are general principals of behaviour and the code of conduct that apply to all situations e.g.: all users need to know what to do if they come across inappropriate material, and that staff members should not give out their personal information to learners such as their personal telephone numbers, email address or allow access to their personal social networking site accounts etc. We must also communicate to children young people and vulnerable groups on courses at Trinity Academy that they should not give out their personal information such as telephone numbers; addresses etc to strangers or publish this information on social networking sites.

A balance needs to be struck between educating staff and learners to take a reasonable approach towards the use of regulation and technical solutions. We must recognise that there are no totally effective solutions to moderate and control the Internet, so this policy incorporates both approaches.

Roles and Responsibilities

Staff

All teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout the Academy and following e-safety procedures. All Academy staff should be familiar with the E-safety and Acceptable use of ICT policy (AUP) as well as their relevance to the Code of Conduct and Safeguarding policies. This is available on the Trinity Academy Network and in hardcopy in the Reception Safeguarding Policies Folder.

- All staff should participate in any e-safety training and awareness raising sessions
- All staff should have read, understood and accepted the Staff Acceptable Use Agreement
- Act in accordance with the AUP and E-Safety Policy
- Staff should report any suspicion of misuse to the Designated Persons or line manager
- Staff should refrain from making negative comments about learners and Trinity Academy on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the Academy and/or lowers morale.
- Staff should help educate learners in keeping safe especially with vulnerable groups.

  Whilst regulation and technical solutions (such as filtering systems) are important, they must be balanced with educating learners to take a responsible approach. The education of learners in e-safety is an essential part of using technology in classes. Staff should act as a good role model in their own use of ICT.
- Where Internet use is pre-planned in sessions or enrichment activities, learners should be directed to sites which are appropriate for their use and procedures should be followed for reporting any unsuitable material that is found on Internet searches. Where practicable staff should pre-check sites and any possible searches.
- Where learners are able to freely search the Internet staff should be vigilant in monitoring the content of websites in case there is any unsuitable material.
- Staff should be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through the use of forums on the VLE/Ondrive and social networking sites, or via internal class emails or text messages on mobile phones

etc, which can cause hurt or distress.

- Learners should be taught to be critically aware of the materials/content they can access online and be guided to validate the accuracy of information.
- Learners are educated to of the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the Internet.

Learners

The provision of ICT resources and facilities are a privilege, not a right. Learners are encouraged to access various technologies in sessions, private study and in the completion of assignments and independent research, and are therefore expected to follow the Academy's AUP. They should participate fully in e-safety activities and report any suspected misuse to a member of staff. Learners are required to sign an agreement to state that they agree to the terms of our AUP and their e-safety responsibilities:

Learners & Staff are expected to:

- Behave in a safe and responsible manner
- Treat equipment with respect
- Be polite and not use e-mail, social media or blogs etc to make negative comments, bully or insult others
- Use the resources only for educational purposes

Learners & Staff are expected not to:

- Waste resources including Internet and printers
- Eat or drink in the ICT suites
- Use someone else's login details or share your own
- Have any inappropriate files (e.g. copyrighted or indecent material)
- Attempt to circumvent or "hack" any systems
- Use inappropriate or unacceptable language
- Reveal their personal details or passwords
- Visit websites that are offensive in any way
- Use chat rooms or newsgroups.
- Do anything that could damage the reputation of the Academy
- Download anything inappropriate or install any programs

Breaching these Rules may lead to:

- Withdrawal from the Academy ICT facilities
- Temporary or permanent prevention of access to the relevant pages on the Internet
- Limited or disabled rights where systems are relevant.
- Appropriate disciplinary action. In the case of students of this Academy, the Academy's Behaviour Policy may be invoked.
- Users should note that breaches of the provisions set out in these Rules may lead to criminal or civil prosecution.

Senior Management Team

The senior management team at Trinity Academy takes e-safety very seriously and will ensure that policies and procedures are in line with best practice and the safeguarding agenda. In particular, they will ensure that all staff receives suitable training and development to carry out their e-safety roles and sufficient resources are allocated to the task. Senior managers will follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff and ensure that there is a robust system in place for monitoring e-safety. This includes making sure that the Academy's Network infrastructure is safe and secure and those policies and procedures approved within this policy are implemented. Regular review of the issues will take place at the ICT Focus

Group meetings with feedback sessions scheduled to the senior management team meetings.

Responding to issues

It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the Academy community are aware those incidents have been dealt with.

Any concerns around the misuse of ICT must follow the referral process within the Safeguarding Policy and Procedure where there is a potential threat to another learner, vulnerable person or member of staff. Any suspected misuse must be reported to a member of staff and then an appropriate course of action will be agreed.

Where it is suspected that any misuse might have taken place by a member of staff will depend on the nature of the misuse and Trinity Academy's disciplinary procedure will be invoked.

Where an allegation has been made against a learner an investigation will take place by the designated persons of the ICT Focus Group. The outcome of the investigation will decide what will be the appropriate course of action and depending on the nature of the misuse the learner could be suspended from classes till the investigation is complete. Should the allegation be found to be true, the sanction will depend on the seriousness of the misuse and whether it was accidental or deliberate, a first time offence, thoughtless or malicious e.g. intended to cause harm to others. Sanctions could involve the learner having ICT access removed for a period of time or in very serious cases, exclusion. Where there is a potential legal issue the Head of School will decide on the need for involvement of outside agencies including the police, together with the designated persons and Senior Management team in line with our Safeguarding and other policies.

Trinity Academy Guest Wi-Fi Network

Trinity Academy provides a guest wireless network which is available to all teaching and non- teaching staff (including volunteers, suppliers, contractors and temporary staff). Use of this provision is governed by the Academy's E-safety and Acceptable Use Policy and by logging onto the network the user is deemed to have agreed to abide by Trinity Academy's Acceptable Use Policy.

All users utilising the guest wireless connection should be aware of and agree to conditions of use including but not limited to the following:

- Trinity Academy assumes no responsibility for the safety of equipment or device configurations, security, or data files resulting from connection to the Academy's guest wireless network or the Internet, nor liability for any damages to hardware, software or data, howsoever caused.
- Guest wireless access is provided as a free service on an "as is" basis with no guarantee of service.
- Users are responsible for setting up their own equipment to access the guest wireless network. A guide is available to help users connect to the guest wireless network.
- Staff cannot assume any responsibility for personal hardware configurations, security or changes to data files resulting from connection to the guest wireless network. It is recommended that users make a backup copy of any settings before configuring their equipment for use on the guest wireless network.
- Use of the guest wireless internet connection is undertaken at the user's own risk.

The wireless network protects users against basic malware/botnet/phishing protection; however, it is the responsibility of the user to protect their wireless devices through use of up-to-date virus protection, personal firewall and any other suitable measures.

- The guest wireless network may be subject to periodic maintenance and unforeseen downtime.

- The Academy filters ALL Internet access.
- Printing access is not available via the guest wireless network. If the user desires to print, they will have to make their own suitable alternative arrangements.
- Any attempt to circumvent Academy procedures or any unauthorised attempt to access or manipulate Academy equipment or networks, may result in permanent disconnection from the guest wireless network and further disciplinary action being taken.

Academy website

- The contact details on the website should be the academy address, email and telephone number. Staff or pupils' personal information must not be published
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. you could replace '@' with 'AT')
- The Chief Executive officer will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the academy's guidelines for publications including respect for intellectual property rights and copyright

Publishing Learner's work or images.

- Images that include learners will be selected carefully and will not provide material that could be reused
- Learner's full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers must be obtained before images of Learners are electronically published
- Learner's work can only be published with their parent's permission, (see Appendix VI)

Mobile Phones

Mobile phones are now a feature of modern society and most of our learners own one. The technology of mobile phones has developed such that they now have the facility to record sound, take photographs and video images. Therefore the academy also recognises the advantages mobile phones have as a ubiquitous learning tool. However, this new technology is open to
abuse leading to the invasion of privacy.

Increasing sophistication of mobile phone technology presents a number of issues for academys:

- They are valuable items that may be stolen
- The integration of cameras into phones leading to potential child protection and data protection issues
- The potential to use the phone e.g. for texting whilst on silent mode
- Inappropriate messages being sent via SMS, including Cyberbullying and sexual harassment
- Interruption to lessons and disrupting the learning of others

- Dependent upon site, phones must always be switched off/put on silent and put away whilst in the classroom. If a learner needs to contact his/her parents/guardians they

will use an academy phone in the main office

- If parents need to contact children urgently they should always phone the academy office
- Academy accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile phones
- It is the responsibility of parents and learners to ensure mobile phones are adequately insured
- Dependent upon site, if a learner breaches these rules they may be liable to a sanction, which could ultimately lead to the pupil signing a 'mobile phone' contract. This involves the learner handing in the device at the start of the day and it being returned at the end of the day.

Laptops/Tablets

- Staff provided with a laptop/tablet purchased by the academy can only use it for private purposes at the discretion of the CEO. Such laptops/tablets remain the property of the academy and are open to scrutiny by senior management, contracted technicians and the ICT
  subject leader
- Laptops/tablets belonging to the academy must have updated antivirus software installed and be password protected
- Staff intending to bring personal laptops/tablets on to the academy premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop.
- Staff should not attach personal laptops/tablets to the academy network.
- The security of academy laptops/tablets is of prime importance due to their portable nature and them being susceptible to theft
- See Academy Laptop/tablet policy (Appendix IV)

Trinity Academy Newcastle

AUP for Staff

ICT and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within academy. To ensure that all adults within the academy setting are aware of their responsibilities when using any form of ICT all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provides positive role models to learners for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the academy equipment in an appropriate manner and for professional use in accordance with the e-Safety Policy
- I will not share my username, password or personal information with anyone else
- I will not leave my computer unlocked, if away from my desk
- I will not give out personal information (mobile phone number, personal e-mail address etc) to learners or parents
- I know I should not use my personal phone to make calls to parents
- I will only use the approved, secure e-mail system (name@trinity.newcastle.sch.uk) for any academy business
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I know that memory sticks are not allowed to be used on academy computers. If I require work to be transferred via memory stick, I can ask the technician to do so.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure academy data is stored securely and used appropriately in accordance with academy and other relevant policies
- I will report any accidental misuse of academy ICT, or accidental access to inappropriate material, to the ICT Subject Leader or Head of School Business
- I will not connect any personal device (laptop/tablet, digital camera etc), to the academy network without authorisation from the Head of School Business
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Head of School Business
- Academy equipment should not be used for any personal social networking use.
- Staff must not accept friendships from Learners on personal social network accounts
- Staff must not accept friendships from pupil/ex-pupil under the age of 25 on personal social networking accounts.
- Social Networking applications should not be used to publish any content, which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal,

sexual or offensive nature that may bring the academy into disrepute.

- Postings should not be critical or abusive towards the academy, staff, Learners or parents or used to place a pupil, staff, or parent at harm.

- Ensure that that the appropriate security/privacy levels are set. Consider all the privacy/security settings available across all aspects of the service – including photos, postings, photographs, bio, etc. Failing to set appropriate privacy levels could result in messages, which are defamatory, libelous or obscene appearing on your profile before you have a chance to remove them.

- I will ensure that my online activity, both in and outside academy, will not bring myself or the academy into disrepute (this includes postings on social networking sites e.g. Facebook)

I have read, understood and agree to this code of conduct. I will support the safe and secure use of ICT throughout the academy. I am aware I may face disciplinary action if I fail to adhere to it.

Signature: _____ Date: _____

Print Name: _____

Trinity Academy Newcastle

Code of Conduct for Learners

I agree to follow these rules when using the Internet:

- I will not share my username, password or personal information with anyone else
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I will not look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this I will tell a teacher immediately
- I will only upload materials which are free from copyright and suitable for academy use
- I will not deliberately misuse or deface other users' work on the academy network/Onedrive or Virtual Learning Environment (VLE)
- I understand that if I intentionally misuse the Onedrive/ VLE I will lose my access privileges.
  Further action may also be taken in line with academy and Local Authority Policy
- I know that my use of the Internet is monitored and further action may be taken if a member of academy staff is concerned about my safety
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- **DENEVIEW STUDENTS:** I will hand in my phone to the main office before the start of the academy day and collect it at the end of the day
- **OAKFIELD STUDENTS:** During lessons I will ensure my phone is switched off.
- I will only play on age appropriate games when given the privilege during class time
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Signed: _____

Class: _____

Date: _____

Trinity Academy Newcastle

Supporting Letter

Dear Parent / Carer

As part of an enriched curriculum your child will be accessing the Internet; viewing websites, using email and the academy Onedrive/ Virtual Learning Environment (VLE).

In order to support the academy in educating your child about e-Safety (safe use of the Internet). Please read and discuss the e-Safety rules attached with your child then sign and return the slip below.

Should you have any concerns and wish to discuss the matter further please contact The Head of School via the academy office.

Yours Sincerely

Bill Curley
Chief Executive Officer

E-Safety Acceptable Use Rules Reply Slip

I have read and discussed the rules with _____ (child's name) and confirm that he/ she has understood what the rules mean and agrees to follow the e-Safety rules to support the safe use of ICT at Trinity Academy.

Parent/ Carer Signature: _____

Print name: _____

Date: _____

Laptop/Tablet Policy
for Staff

Staff provided with a laptop/tablet purchased by the academy, agree to the following terms of use:

1 The laptop/tablet remains the property of Trinity Academy and is for the use of the person it is issued to and must be returned to the academy if and when the teacher leaves employment at the academy.

2 The laptop/tablet is open to scrutiny by senior management, contracted technicians and the ICT Subject Leader at academy.

3 Insurance cover: It will be important to check with insurers that equipment to be taken off the premises is covered and you are satisfied on the level of any excess to be paid in the event of a claim. (Individual staff home contents insurance policies may apply- please note that most policies will not cover theft from cars).

4 Acceptable Use – teachers must accept and adhere to the academy's AUP.

5 The loading of additional software must be authorised by the academy, support teaching and learning and be compliant with the following regulations:

- **Copyright, Designs and Patents Act 1988**
  Specifies that all software must be used only in accordance with the terms of the license. Generally, the making of copies is forbidden and is a criminal offence.
- **Computer Misuse Act 1990**
  Identifies three main offences concerning unauthorised access to systems, software or data.

Please speak to your academy before loading any software

6 Anti-Virus software must be installed and should be updated on a regular basis. Academy ICT staff will advise on the routines and schedule of this operation. Sophos anti-virus updates are available from academy and are covered by the Local Authority license.

7 All repair and maintenance of laptops/tablets must be conducted under the terms and conditions of the warranty.

8 Data Protection – the terms of the academy's Data Protection registration should be adhered to and users must clearly understand that there is a personal legal duty on them as well as the academy.

9 Any charges incurred by users accessing the Internet from home are **not** chargeable to the academy.

10 Staff should not connect personal laptops onto the academy network.

11 Failure to comply with these guidelines and the academy's AUP, may result in the withdrawal of the laptop and may lead to disciplinary proceedings.

Laptop Details:

Make: _____

Model: _____

Serial Number: _____

Authorised by Chief Executive Officer

Signed: _____

Date: _____

Member of Staff:

Print name: _____

Signed: _____

Date: _____

DENEVIEW

Mobile Phone Policy

- Trinity Academy discourages Learners from bringing mobile phones to academy
- The phone must be clearly labelled with the child's name, switched off and given in to the office on arrival at academy
- Where a pupil is found with a mobile in academy, including the playground, the phone will be taken from the pupil and placed in the office. Parents will be contacted to collect the phone

OAKFIELD

- If a pupil is found taking photographs or video footage with a mobile phone of either Learners or teachers, this will be regarded as a serious offence and the Chief Executive Officer will decide on appropriate disciplinary action. In certain circumstances, the pupil may be referred to the Police. If images of other Learners or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by an appropriate person
- Parents are advised that Trinity Academy accepts no liability for the loss or damage to mobile phones which are brought into the academy
- If a pupil needs to contact his/her parents/guardians they will be allowed to use a academy phone. If parents need to contact children urgently they should phone the academy office and a message will be relayed promptly

This policy became operational from November 2013
and Reviewed on an annual basis.
The policy may be amended from time to time in accordance with academy development and any changes to legislation.

Trinity Academy Newcastle

Photographs of Children – Parental Consent Form

Name of Child: _____ Date of Birth: ___/ ___/ ___

Trinity Academy would like to take photographs and or video recordings of Learners whilst they attend the academy to celebrate their achievements and successes. Still or moving images may be published in our printed publications (e.g. Academy prospectus, newsletters) and/or on our external website (www.trinity.newcastle.sch.uk). They may also be used to promote the good educational practice of the academy to other teachers e.g. at training events organised by the Local Authority or national education/government institutions. Childrens' names will never be published alongside their photographs externally to the academy. Names may be used internally, for example – on a display.

Photographs / videos may also be published for internal use only, as part of children's regular classroom work e.g. on classroom displays, within multimedia projects (e.g. PowerPoint), on the academy's internal network and to share educational achievements with parents e.g. video presentation of an academy trip. Electronic images, whether photographs or videos, will be stored securely on the academy's network which is accessible only by authorised users. Before using any photographs/videos of your child we need your permission. Please answer questions 1 to 5 below, then sign and date the form where indicated.

Please return the completed form to the academy office as soon as possible.

[Please delete]

1. May we use your child's photograph in printed publications produced by Trinity Academy or Newcastle Local Authority?
   Yes / No

2. May we use your child's photograph on our Internet website
   a) as part of a large group or whole academy activity?
   Yes/No

   b) showing an individual activity? (e.g. holding a winner's trophy)
   Yes / No

3. May we allow your child's photograph (e.g. as part of a academy team or record of a academy event) to be used for publication in a newspaper?
   Yes / No

4. May we use any photograph or video of your child internally as part of the regular curriculum and work of the academy?
   Yes / No

5. May we use any video containing your child to share good educational practice with teachers from other academies?

Yes / No

This form is valid from the date of signing until your child leaves the academy. Photographs and videos may be securely archived after your child has left the academy but will not be re-used or re-published externally without renewed consent. Archiving provides a valuable record of the academy's history for future generations.

Please note, we DO NOT allow any parents/carers to record (photo/video) events.

Signed: _____ Date: _____

Print name: _____

Trinity Academy Newcastle

Video of Children – Parental Consent Form

Your child has been selected for inclusion in a video, which the following organisation wishes to take on the date(s) shown:

Organisation:

_____

Date video to be taken:

_____

The purpose(s) for which the video is to be taken:

_____

This will be displayed in the following places (must clearly state “Internet address” if it is intended to publish via this medium):

_____

If you have any queries regarding use of the video or change your mind then please contact the above organisation at the following address:

_____

Declaration

Being the parent or person responsible, I grant permission for a video of my child to be used in printed and electronic (delete as appropriate) publicity materials generated by the organisation named above. I acknowledge that the video will only be used for the purpose(s) stated and that I have a right to change my mind.

Name of Child: _____

Academy: _____

Academy year: _____

Your Name: _____

Signature: _____ Date ___/ __ / ___

Child’s Signature: _____ Date ___/ __ / ___
(if over 12 years)

Appendix VIII

E-Safety Policy Checklist

An AUP should follow some general principles, summarised in the following ten points.

1. **Be clear and concise** - Aim for an A4 page or two of core rules, issued as part of the home-academy agreement or induction programme. You can supply more detail in a supplementary document.

2. **Be relevant to your setting** - When creating your AUP, consider the needs and characteristics of your users, services and support networks. Bear in mind other policies – such as child protection, anti-bullying and behaviour policies. Ensure your AUP reflects these policies and vice versa.

3. **Encourage user input and ownership** - Involve children and young people, parents and carers and people expected to enforce the AUP in developing and reviewing it. Users are more likely to keep to your AUP if they feel ownership of it.

4. **Write in an appropriate tone and style for users** - Do you need different documents for younger and older pupils, staff, parents and carers, or those with particular communication needs? If so, try and consult with each group and meet their needs (see example AUPs below).

5. **Promote positive uses of all technologies** - Technology offers many wonderful opportunities. Promote the positives in your AUP rather than focusing on the negatives. Remember that technologies are evolving all the time. Reinforce the concept of safe and responsible use of all technologies in your AUP rather than referring to specific devices.

6. **Outline clearly acceptable and unacceptable behaviours** - Users need to understand clearly what they can (and can't) do online using the technology and services available to them in the learning or care setting. They also need to understand how they can use their own equipment in certain settings. You may choose to ban all personal technology devices, or approve their use in certain situations, or encourage their use to support learning. Whatever you decide, make it clear.

7. **Outline clearly what network monitoring will take place** - Users have a right to know how their network access will be monitored. An open and honest approach can help prevent challenges to authority should e-Safety incidents occur.

8. **Outline clearly the sanctions for unacceptable use** - Users need to understand what penalties they face if they break the rules. These may range from temporary suspension of services to disciplinary action or even legal intervention, depending on the seriousness of the incident.

9. **Review and update regularly** - To remain effective, AUPs must be regularly reviewed and updated. In addition to a regular programme of review, AUPs should be reviewed more often if necessary. For example, as a response to emerging issues or serious e-Safety incidents.

10. **Communicate regularly to all stakeholder groups** - If you want users to keep to your AUP, they need to be aware of it and understand it. Consider the best

approaches for introducing the AUP. Perhaps through the home-academy agreement for Learners and parents or carers, or within induction programmes for staff. Look for opportunities to assess whether the AUP is understood. Reinforce the AUP regularly, monitor its impact and ensure you communicate any changes.

Appendix IX
E-Safety Policy Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the e-Safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator and Chief Executive Officer

Does the academy have an e-Safety Policy?	Y/N
Date of latest update (at least annual):	
The policy was agreed by Governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Management Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator in academy is:	
The e-Safety Coordinator is:	
Has e-Safety training been provided for all Learners(age appropriate) and all members of staff?	Y/N
Is there a clear procedure for responding to an incident or concern?	Y/N
Do all staff sign a Code of Conduct or AUP on appointment?	Y/N
Are all Learners aware of the e-Safety rules or AUP?	Y/N
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the Academy e-Safety rules?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider that complies with DfE requirements?	Y/~~N~~
Has the academy-level filtering been designed to reflect educational objectives and been approved by the SLT?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of the SLT?	Y/N

Appendix X
Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material that is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation, in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, Connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Academys should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with

important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files)
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

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

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.
The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment, it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a license associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a license before you copy or use someone else's material.
It is also illegal to adapt or use software without a license or in ways prohibited by the terms of the software license.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material that is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material, with a view of releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions. This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”

63 (6) must be “grossly offensive, disgusting or otherwise obscene”

63 (7) this includes images of “threats to a person’s life or injury to: anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for academy’s which relate to Cyberbullying/Bullying:

- Head Teachers have the power “to such an extent as is reasonable” to regulate the conduct of Learners off site
- Academy staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the academy behaviour/anti-bullying policy

Signed on behalf of the Governing Body:

_____

Peter Carter (Chairperson of the Board)

Date: 11.10.17

Appendix XI
Further Information and Guidance

CEOP (Child Exploitation and Online Protection Centre
www.ceop.police.uk

Childline
www.childline.org.uk

Childnet
www.childnet.com

Digital Literacy
http://www.digitalliteracy.org.uk/Home.aspx

Safer Internet
http://www.saferinternet.org.uk/

Information Commissioner's Office
www.ico.org.uk

Internet Watch Foundation
www.iwf.org.uk

Kent Primary Advisory e– Safety
www.kenttrustweb.org.uk/kentict/kentict_home.cfm

Kidsmart
www.kidsmart.org.uk
www.netsmatzkids.org

Newcastle Academy's IT Support Team
Help with filtering and network security
Tel: (0191) 277 7282

SWGFL http://www.digital-literacy.org.uk/Home.aspx

Think U Know website
www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse
www.virtualglobaltaskforce.com

BBC
http://www.bbc.co.uk/cbbc/topics/stay-safe

Acknowledgement

We gratefully acknowledge that this guidance is adapted from information provided by Kent Local Authority