The Active Learning Trust

ACTIVE LEARNERS • ACTIVE LEADERS • ACTIVE CITIZENS

ONLINE SAFETY AND ACCEPTABLE USE

Document Control - Policy Amendments

Date	Version	Summary of Changes	Reviewer/s
January 2024	1.0	Initial version adapted from the Key template	Chris Everard, Director of Operations
February 2024	1.1	Added Acceptable Use Agreement for Specialist Settings to appendices Added wording for specialist settings to 3.13, 4.9 and 9.1 Added DSL and senior leadership team to 7.3 Updated section 10.1 to refer to the academy's mobile phone policy Added wording regarding school social media accounts to the staff acceptable use policy (appendix D) Added a statement on guest Wi-Fi to 3.16 Updated 5.2 to refer to parent information evenings Added 'via the school website' to 5.3 Changed 'search and confiscations' policy to 'relevant policies' 6.7 Added email address to contact under 11.4 Added section 12 to refer to the use of staff personal devices	Chris Everard, Director of Operations

Policy Review

Next Review Date:	January 2025
Ratified by:	Trust Board
Date Ratified:	
Dissemination:	The policy will be made available to all Trust employees

Contents

1. Aims

1.1 The trust and its academies aim to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers, trustees and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** - being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

2.1 This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

2.2 It also refers to the DfE's guidance on protecting children from radicalisation.

2.3 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2.4 The policy also takes into account the National Curriculum computing programmes of study.

2.5 This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

The Local Governing Body

3.1 The governing body for each academy has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.2 The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.3 The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

3.4 The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.5 The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

3.6 The governing body must ensure the academy has appropriate filtering and monitoring systems in place on academy devices and academy networks, and will regularly review their effectiveness. They will review the DfE filtering and monitoring standards and discuss with IT staff and service providers what needs to be done to support the academy in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs

3.7 All governors will:

- Ensure they have read and understood this policy
- Agree to adhere to the terms on acceptable use of the academy's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their approach to safeguarding and related policies or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the important of recognizing that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

3.8 The Headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.

The Designated Safeguarding Lead

3.9 The academy's designated safeguarding lead (DSL) and deputies are set out in our safeguarding policy.

3.10 The DSL takes lead responsibility for online safety in the academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on academy devices and academy networks
- Working with the Head of IT to make sure the appropriate systems and processes are in place
- Working with the headteacher, Head of IT and other staff, as necessary, to address any online safety issues or incidents
- Managing online safety issues and incidents in line with the safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the headteacher and/or governing body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Head of IT

3.11 The Head of IT for the Active Learning Trust is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on academy devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at the academy. This includes terrorist and extremist material.
- Ensuring that the academy's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and ensuring the academy's IT systems are monitored on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Working with DSLs to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the academy anti-bullying and behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

3.12 All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet, and ensuring that pupils follow the academy's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by contacting the Head of IT if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents / carers

3.13 Parents / carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet where they are competent to do so

3.14 Parents / carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Cyber Security for families – National Cyber Security Centre

Visitors and members of the community

3.15 Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign Appendix D.

3.16 Visitors and members of the community will be given access to guest WiFi accounts only.

4. Educating children about online safety

4.1 Children will be taught about online safety as part of the curriculum.

4.2 The text below is taken from the National Curriculum computing programmes of study as well as guidance on relationships education, relationships and sex education (RSE) and health education.

4.3 All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary Curriculum

4.4 In Key Stage 1 pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

4.5 Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

4.6 By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules are principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Secondary Curriculum

4.7 In Key Stage 3 pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

4.8 In Key Stage 4 pupils will be taught to:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

4.9 By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognize consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

For pupils with complex needs who attend specialist settings the content above will be taught in accordance with the appropriate developmental age and ability of the individual

4.10 All our academies will:

- Cover the safe use of social media and the internet will also be covered in other subjects where relevant
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND

5. Educating parents/carers about online safety

5.1 The academy will raise parents/carers' awareness of internet safety in letters, newsletters and other communication sent home. Information will also be shared via the academy website. This policy will be shared with parents/carers.

5.2 Online safety will be covered during open evenings and parent information evenings.

5.3 The academy will let parents know via the school website:

- What systems the academy uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the academy (if anyone) their child will be interacting with online

5.4 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5.5 Concerns of queries about this policy can be raised with the headteacher.

6. Cyber-bullying

6.1 Cyber-bullying takes place online, such as through social networking sites, messages apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.3 The academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

6.4 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.5 All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

6.6 The academy also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

6.7 In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy anti-bullying and behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained and dealt with in line with processes set out in the relevant policies.

6.8 The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. Examining electronic devices

7.1 The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils
- Is identified in the academy rules as a banned item for which a search can be carried out
- Is evidence in relation to an offence

7.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above they will also:

- Make an assessment of how urgent the search is, and consider the risk of other pupils and staff. If the search is not urgent they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

7.3 Authorised staff members may examine, and in exceptional circumstances erase any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so once they have checked with the DSL and a member of the senior leadership team

7.4 When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm
- Undermine the safe environment of the academy or disrupt teaching

- Commit an offence

7.5 If inappropriate material is found on the device, it is up to the staff member, in conjunction with the DSL and a member of the senior leadership team, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

7.6 When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person
- The pupil and/or parent/carer refuses to delete the material themselves

7.7 If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council or Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

7.8 Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

8. Artificial Intelligence (AI)

8.1 Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

8.2 The academy recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

8.3 The academy will treat any use of AI to bully pupils in line with our behaviour policy.

8.4 Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the academy.

9. Acceptable use of the internet in the academy

9.1 All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (see appendices), where they are competent to do so. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

9.2 Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

9.3 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

9.4 More information is set out in the acceptable use agreements in the appendices.

10. Pupils using mobile devices in the academy

10.1 Refer to the academy's mobile phone policy

11. Staff using work devices outside of the academy

11.1 All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

11.2 Staff members must not use the device in any way that would violate the academy's terms of acceptable use (see appendices).

11.3 Work devices must be used solely for work activities.

11.4 If staff have any concerns over the security of their device, they must seek advice by raising a ticket with the ICT team at help@activelearningtrust.org.

12. Staff using personal devices for work activities

12.1 Work devices should be used where possible. Where personal devices are used for work activities they should be kept secure and personal or confidential data should not be saved outside of the academy network.

12.2 Personal devices should not be connected to the academy network

12.3 The use of personal mobile devices by staff is covered in the academy's mobile phone policy

13. Responding to issues of misuse

13.1 Where a pupil misuses the academy's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend

on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

13.2 Where a staff member misuses the academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

13.3 The academy will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Training

14.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

14.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

14.3 By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

14.4 Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

14.5 The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

14.6 Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

14.7 Volunteers will receive appropriate training and updates, if applicable.

14.8 More information about safeguarding training is set out in our safeguarding policy.

Appendix A – Acceptable Use Agreement (EYFS and KS1)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the academy's ICT systems (like computers) and get onto the internet in the academy I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use academy computers for academy work only
• Be kind to others and not upset or be rude to them
• Look after the academy ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the academy network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix B – Acceptable Use Agreement (KS2, KS3, KS4, KS5)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the academy's ICT systems (like computers) and get onto the internet in the academy I will:** • Always use the academy's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the academy's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into the academy:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the academy, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in the academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix C – Acceptable Use Agreement (Specialist Settings)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the academy's ICT systems (like computers) and get onto the internet in the academy I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately I select a website by mistake, receive messages from people I don't know or find anything that may upset or harm me or my friends • Use academy computers for academy work only • Look after the academy ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password and never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the academy network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **If I bring a personal mobile phone or other personal electronic device into the academy:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the academy **and it will be handed in to be kept secured and switched off until the end of the day when it is returned** • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Log in to the academy's network using someone else's details **I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix D – Acceptable Use Agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the academy's ICT systems and accessing the internet in the academy, or outside the academy on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the academy's reputation • Access social networking sites or chat rooms, unless it is a school account and I have permission to do so as part of my role • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network • Share my password with others or log in to the academy's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the academy, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the academy • Access the academy network using a personal device	
I will only use the academy's ICT systems and access the internet in the academy, or outside the academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the academy's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**