SUMMIT
LEARNING TRUST

Online Safety & AUP Policy

Approved by:	Board of trustees	**Date:** September 2023
Last reviewed on:	September 2023	
Next review due by:	September 2025	
Monitoring & Review	Board of Trustees	
Links	Safeguarding and Child Protection Policy, Behaviour Policy, Disciplinary Policy, GDPR Data Protection Policy and Privacy Notices, Complaints Policy, Staff Code of Conduct	
Staff responsible	IT Director, Principals, All staff members	

Contents

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of learners, staff members, volunteers, trustees and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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, anti-Semitism, 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools and colleges 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
- Meeting digital and technology standards in schools and colleges

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

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 learners' electronic devices where they believe there is a 'good reason' to do so.

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

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

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for approving this policy every 2 years.

3.2 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The LGB should ensure that all members of staff undergo safeguarding and child protection training (including awareness of online safety which, amongst other aspects, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring). For all learner facing members of staff, specific online training is mandatory.

The LGB will co-ordinate regular meetings with appropriate staff members to discuss online safety and monitor online safety logs as provided by the academy's designated safeguarding lead (DSL).

All governors and Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some learners with SEND because of the importance of recognising 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

3.3 The Principal

The Principal is responsible for ensuring that staff members and volunteers understand this policy, and that it is implemented consistently throughout the academy.

3.4 The Designated Safeguarding Lead (DSL)

Details of the academy's Designated Safeguarding Lead (DSL) are set out in our Safeguarding and Child Protection Policy and safeguarding strategy on each academy's website.

The DSL takes lead responsibility for online safety (including understanding the filtering and monitoring systems and processes in place) in each academy, in particular:

- Supporting the Principal in ensuring that staff members and volunteers understand this policy and that it is being implemented consistently throughout our Trust
- Working with the Principal, Summit Central IT Team and other staff members, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy's Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring appropriate filtering and monitoring systems are in place
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy's Behaviour Policy
- Updating and delivering online safety training to relevant staff members, volunteers, governors and trustees. (appendix 4 contains a self-audit for staff members, volunteers, governors and trustees on online safety training needs)

- Ensuring teachers and educational support staff are knowledgeable in providing learners with online preventative education
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the Principal and/or LGB

This list is not intended to be exhaustive.

3.5 The Central IT team

The Central IT team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners and staff members are kept safe from potentially harmful and inappropriate content and contact online while at school / college, including terrorist and extremist material
- Ensuring that each academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring each academy's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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's Behaviour Policy

This list is not intended to be exhaustive.

3.6 All staff members, volunteers, governors and trustees

All staff members, volunteers, governors and trustees including contractors and agency staff 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 (appendix 3), and ensuring that children and young people follow the academy's terms on acceptable use (appendices 1, 2 and 2a)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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's 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'
- Completing all training provided by the DSL, wider safeguarding team, Edtech team and external services.

This list is not intended to be exhaustive.

3.7 Parents and Carers

Parents and carers are expected to:

- Notify a member of staff or the Principal 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 (appendices 1 and 2)
- Advise their child on how to keep safe online in accordance with relevant laws and guidance.

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

Support for learners

Childline for free and confidential advice

UK Safer Internet Centre to report and remove harmful online content

CEOP for advice on making a report about online abuse

Support for Parents and Carers

National college Training and Resources platform

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provides independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Educate against hate provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Parentzone provides help for parents and carers on keeping their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

3.8 Visitors and members of the community

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 (appendix 3).

4. Educating learners about online safety

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

All schools have to teach:

- **Relationships Sex and Health Education**

In **Key Stage 1**, learners 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

Learners 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

By the **end of primary school**, learners 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 and 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 a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, learners 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

Learners in **Key Stage 4** will be taught:

- 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

By the **end of secondary school**, learners 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 which 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 recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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 learners with SEND.

Academies will use assemblies to raise learners' awareness of the dangers that can be encountered online and may also invite speakers to talk to children and young people about this.

5. Educating parents and carers about online safety

Academies will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents and carers.

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

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Online Safety Incidents

6.1 Definition

Online safety incidents encompass a wide range of negative interactions and activities that occur on the internet, including but not limited to social networking sites, messaging apps, or gaming platforms. These incidents involve any repetitive and intentional harm inflicted upon one person or a group by another person or group in an online environment, where there may be an imbalance of power or a violation of acceptable online behaviour. (See also the academy's Behaviour Policy.)

6.2 Preventing and Addressing Online Safety Incidents

To promote online safety, we are committed to ensuring that learners understand what constitutes an online safety incident and how to respond when they encounter such situations, whether as victims or witnesses. Learners will be informed about the reporting mechanisms available and encouraged to report any incidents they come across.

The academy will actively engage with learners to discuss online safety incidents, shedding light on the reasons behind their occurrence, the various forms they can take, and the potential consequences. Class teachers and form teachers will address online safety incidents within their respective groups, and these issues will also be covered in assemblies.

Teaching staff are encouraged to integrate discussions about online safety incidents into the curriculum, including areas like personal, social, health, and economic (PSHE) education, as well as other relevant subjects such as computing.

All staff members, governors, volunteers, and trustees (where applicable) will receive general guidance on online safety incidents, their impact, and how to support learners as part of safeguarding training (see section 11 for more detail). For all learner facing members of staff, specific online training is mandatory.

The academy will provide information and leaflets on online safety incidents to parents and carers, ensuring they are aware of the signs to look out for, how to report incidents, and how to support children who may be affected.

In response to a specific online safety incident, the academy will follow the procedures outlined in the academy's Behaviour Policy. In cases involving illegal, inappropriate, or harmful content shared among learners, the academy will make all reasonable efforts to contain the incident.

The Designated Safeguarding Lead (DSL) will assess whether incidents involving illegal material should be reported to the police and, if necessary, collaborate with external services to address the situation.

6.3 Examining electronic devices

Academy staff members have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on learners' electronic devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff members must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

** Staff members may also confiscate devices for evidence to hand to the police, if a learner discloses that they are being abused and that this abuse includes an online element.*

Any searching of children and young people will be carried out in line with:

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

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet

All learners, parents, carers, staff members, governors, trustees, volunteers and visitors are expected to read and agree to the terms of the acceptable use of the Trust's ICT systems and the internet.

Use of the Trust's internet should be for educational purposes and the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners, staff members, volunteers, governors, trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

8. Learners using personal devices

Use of personal devices is governed by each academy's Behaviour Policy.

Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the academy's Behaviour Policy, which may result in the confiscation of their device.

9. Staff members using devices outside of academies

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

<u>All devices</u>

- 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)
- All devices and external storage such as memory sticks and flash drives containing data relating to the academy/Trust must be encrypted.
- Only Trust approved Cloud systems eg Office 365/Teams/OneDrive, should be used to view, share or store academy/trust data.
- Use of Multi Factor Authentication is mandatory for all members of staff on Trust approved Cloud Systems where applicable.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- When working with sensitive personal data, avoid positioning screens in a way they can be easily read by other people

<u>Academy devices</u>

- Always keep academy devices secure; whether in class, around the academy, in transit or at home.
- Ensure all academy devices are logged off at the end of the working day.
- Only academy devices may be used to take and store images of learners. You must ensure you have the appropriate consents beforehand.

<u>Personal devices</u>

- Never use a personal device to take or store images of learners.
- You may use a personal device to access academy systems for work purposes where necessary. In the interests of a healthy work/life balance, you are not expected to do so after working hours. But you must never save any work-related personal data files to that device.

<u>Networks</u>

- Never logon to public Wi-Fi networks and never use public computers, such as in public libraries, while working with work-related personal data.
- Avoid taking personal data off-site whenever possible. Access it remotely by using the secure systems that have been approved by the Summit Central IT Team instead.

Staff members must not use the device in any way which would violate the academy's terms of acceptable use.

For additional information please refer to the **Data Protection Guidance for Staff** on the GDPR section of the Summit Learning Trust portal.

If staff members have any concerns over the security of their device, they must seek advice from the Trust Central IT Team.

10. How the academy will respond to issues of misuse

Where a learner misuses the academy's ICT systems or internet, we will follow the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member, volunteer, LGB or trustee 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 appropriate disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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).

In addition to this, all staff members receive mandatory cybersecurity training to raise their awareness of potential online risks and to equip them with the knowledge and skills needed to protect sensitive information, maintain data integrity, and adhere to relevant laws and regulations. This training ensures that everyone in the organisation is actively contributing to a secure and compliant online environment.

The DSL and deputy/deputies 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.

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

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the Trust DSL in consultation with academies DSLs and the Director of IT. At every review, the policy will be shared with the governors and the updated policy will be uploaded to the Trust website.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Disciplinary Policy
- Data Protection Policy and Privacy Notices
- Complaints Policy
- Staff Code of Conduct
- Data Protection Guidance for Staff

Appendix 1: EYFS, KS1 and KS2 acceptable use agreement (learners, parents and carers)

All academy devices require users to click on the acceptable use policy agreement button before they can be used. The agreement is:

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS, PARENTS AND CARERS

Name of child:

When I use the school’s ICT systems and get onto the internet in school 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 click on a website by mistake
    - I receive messages from people I do not know
    - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school 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
- 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
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (child):	**Date:**

Parent or carer agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school’s ICT systems and internet and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: KS3 and KS4 acceptable use agreement (learner, parents and carers)

All academy devices require users to click on the acceptable use policy agreement button before they can be used. The agreement is:

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS, PARENTS AND CARERS

Name of child:

I will read and follow the rules in the acceptable use agreement policy

When I use the school’s ICT systems and get onto the internet in school I will:

- Always use the school’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 username 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 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 have 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
- Log in to the school’s network using someone else’s details
- Arrange to meet anyone offline without first consulting my parent or carer, or without adult supervision

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (learner):	**Date:**

Parent/carer’s agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: KS5 acceptable use agreement (learners)

All academy devices require users to click on the acceptable use policy agreement button before they can be used. The agreement is:

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS

Name of learner:

I will read and follow the rules in the acceptable use agreement policy

When I use the college's ICT systems and get onto the internet in college I will:

- Always use the college's ICT systems and the internet responsibly and for educational purposes only
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times
- Tell a teacher 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 have 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
- 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)
- Install any unauthorised software, or connect unauthorised hardware or devices to the college's network
- 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
- Log in to the college's network using someone else's account.

I agree that the college will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (learner):	**Date:**

Appendix 4: acceptable use of ICT for staff members, volunteers, governors and trustees

ACCEPTABLE USE OF THE ACADEMY’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF MEMBERS, GOVERNORS, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/governor/trustee/volunteer/visitor:

When using the academy’s ICT systems and accessing the internet within an academy, or outside an 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
- 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 learners without checking with teachers first
- Share confidential information about the academy, its learners or staff members, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the academy

I will only use the academy’s ICT systems and access the internet in academy, or outside 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 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 learner 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 learners in my care do so too.

Signed (staff member/governor/trustee/volunteer/visitor):	**Date:**

Policy for the Acceptable Use of ICT

By accepting use of a Summit Learning Trust ICT device, I agree that I will:

- Report any accidental damage immediately to Trust IT Support

- Have due regard to, and comply with, the academy's policy of Acceptable Use of Email and the Internet (as detailed in the attached document)

- Return the device at the end of my term of employment to the Summit Central IT team. The device may also need to be returned during any periods of extended leave, e.g. parental leave, long term illness, secondment etc.

- Ensure that any applications downloaded are suitable and in line with the correct usage of email and the internet policy

- Ensure that the device is always kept securely, within academies, during transit and at home and accept that the cost of any avoidable accidental damage may be charged back to my faculty

- Take good care of the device

Policy for the Acceptable Use of email and the Internet

The policy set out in this document is that which has been agreed for the acceptable use of the Internet within all Summit Learning Trust academies. All the guidelines have been produced in the light of current legislation including the following Acts:

- **Copyright, Designs and Patent Act (1988)**
- **Human Rights Act (1998)**
- **Regulation of Investigatory Powers Act (2000)**
- **Data Protection Act (2018)**

PART 1 – INTRODUCTION

1.1 Purpose

This is a corporate statement of good computer practices to protect Summit Learning Trust academies from casual or intentional abuse. With the growth in use of e-mail and access to the internet throughout the organisation, there are a number of threats and legal risks to the academies, as well as the potential costs of time wasting, that can be avoided by following the practices outlined.

1.2 Scope

These guidelines apply to any members of staff who use Summit Learning Trust systems.

1.3 Publicising the guidelines

Effective communication is vital to increase staff member awareness of these guidelines and their use within Summit Learning Trust academies. All users will be notified of the policy for the acceptable use of email and the internet, and the policy will be made available electronically.

New starters should not be given access to e-mail or the internet until they have seen and accepted these policies.

Any major revisions to these policies or guidelines will be notified via e-mail.

1.4 Monitoring

Summit Learning Trust has filtering software and systems in place to monitor all device and Internet usage, and these will be checked and analysed on a regular basis. Certain sites will be blocked if they are deemed to hold inappropriate or explicit material.

Although Summit Learning Trust respects the privacy of every individual throughout the organisation, all communications (both incoming and outgoing) will be checked for content and attachments to always make sure that the security and integrity of our Trust is not breached. The sender of any message that is intercepted will be notified immediately.

1.5 Disciplinary Process

Action will be taken in line with the Trust’s Disciplinary Policy against users found to have breached the policies outlined in these guidelines. Certain circumstances may be classed as gross misconduct and may lead to dismissal.

PART 2 – RESPONSIBILITIES

2.1 Board of trustees & LGB (Local Governing Body)

The policies and these guidelines have been approved and adopted by the Board of trustees and LGB (Local Governing Body)

2.2 Managers and Team Leaders

It is the responsibility of all managers and team leaders that the policies and guidelines are properly implemented and policed.

2.3 Summit Central IT Team

The Summit Central IT Team will monitor Internet communications with monitoring and filtering software. The appropriate security virus and malware prevention mechanisms will be maintained and updated to meet the ongoing requirement of all academies.

2.4 Members of Staff

All staff members with access to Summit Learning Trust systems will be held responsible for complying fully with the academy/Trust computer policies and guidelines.

PART 3 – IT SYSTEMS USAGE GUIDELINES

3.1 Confidentiality

Messages sent and received via the internet are regarded by the Companies Act as having the same legal status as a corporate letter. Any material viewed as highly confidential or valuable to the academy or Trust should not be emailed externally.

A disclaimer document will be attached to all e-mails with an individual signature for each user. In no instance should the disclaimer be tampered with, although the signature can be altered.

It should be remembered that the internet does not guarantee delivery or confidentiality.

It should be noted that there are systems in place that monitor IT systems and their usage.

Analysis of this information may be given to managers if thought appropriate. No user should have any expectation of privacy.

3.2 Etiquette

Users should always use appropriate etiquette when authoring communications such as emails.

In some instances, where the nature of a message may be deemed confidential, it may be appropriate to notify, or even seek permission from, the original sender before forwarding a message onto another recipient.

3.3 Inappropriate behaviour

Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations.

Messages should not contain material or language that could be viewed as offensive to others or as contravening the academy Equal Opportunities Policy.

3.4 Security

All Trust internal systems are protected by comprehensive security solutions.

In order to prevent security breaches, users are advised not to open any unsolicited email attachments, click unverified hyperlinks or independently load any software onto Trust devices.
If a user inadvertently causes a security breach they need to contact the Summit Central IT Team via the Help Desk (https://summitlearningtrust.freshdesk.com) immediately and follow guidance.

3.5 Housekeeping

Emails are retained for 3 years in accordance with Trust policies.

Emails and attachments, incoming or outgoing through the firewall, are limited to 25MB but good practice is that file attachments should only be sent to a minimum of recipients and if they are large files.

3.6 Respecting copyright

Staff members with internet access must comply with the copyright laws of all relevant countries. Users must not intentionally download any material that holds a copyright notice. This also relates to downloading and copying unlicensed software.

3.7 Rules for business use

Staff members should always check with the Summit Central IT Team before downloading and installing any software on Trust devices. Downloaded software needs to be properly licensed and registered. There are systems in place to monitor all computer and internet usage including any software downloads.

It is your responsibility to ensure that confidential information is not readily visible to other parties and your computer should be locked whilst you are away from your workspace.

Appendix 5: online safety training needs – self-audit for staff members, volunteers, governors and trustees

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in your academy?	
Are you aware of how learners can abuse their peers online?	
Do you know what you must do if a learner divulges a concern or issue with you?	
Are you familiar with the academy's acceptable use agreement for staff members volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for learners, parents and carers?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training or further training?	

Appendix 6: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**