Online Safety Policy

Approved by:	Board of Trustees	**Date:** July 2019
Last reviewed on:	July 2019	
Next review due by:	July 2021	
Monitoring & Review	Board of Trustees	
Links	Child protection and safeguarding policy, Behaviour policy, Staff disciplinary procedures, GDPR Data protection policy and privacy notices, Complaints procedure	
Staff responsible	ICT Director, Principals	

Contents

1. Aims

Our School aims to:

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

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 on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The Local Governing Body

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

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

All governors/Schools will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the School's ICT systems and the internet (appendix 2)

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the School.

3.3 The designated safeguarding lead

Details of the School's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy and safeguarding strategy and on the School website. Details of the school's safeguarding lead are set out in the school safeguarding policy and on the school website.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the School
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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 School behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the Principal and/or LGB
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.4 The ICT support team

The ICT support team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at School, including terrorist and extremist material
- Ensuring that the School's and school'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 the School's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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 School's and school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the School's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents 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 School's and school's ICT systems and internet (appendix 1)
- It is parents' responsibility to advise their child how to keep safe online, and to ensure this safety out of school hours.

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the School'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 2).

4. Educating pupils about online safety

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

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

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

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

Pupils 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

Schools will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

If parents 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. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School behaviour policy.)

6.2 Preventing and addressing cyber-bullying

Adapt this sub-section to reflect your school's approach.

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.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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

In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL will ensure **all matters are promptly reported to the police where illegal material is involved,** and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff 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 pupils' electronic devices, including mobile phones, iPads and other tablet 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 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 school rules

If inappropriate material is found on the device, the staff member must report the matter to the DSL promptly or in the DSL's absence to a member of the senior leadership who will follow the appropriate procedures.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school/the School must not install any unauthorised software on the device and must not use the device in any way which would violate the school's/School's terms of acceptable use, as set out in appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school/the Trust. Any USB devices containing data relating to the school/Trust must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT support team.

Work devices must be used solely for work activities.

10. How the School will respond to issues of misuse

Where a pupil misuses the school'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 misuses the school'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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School 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 cyber-bullying and 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).

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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 2 years by the School DSL in consultation with school DSLs and the Director of ICT. At every review, the policy will be shared with the LGB and the updated policy will be uploaded to the school website.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (pupils and parents/carers)

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

- **You will only use applications and websites that are relevant to your study, are legal and which will not cause offence to others**
- **You will keep your username and password private and never pass it on to others. You will never use anyone else's username or password**
- **You will understand that the Trust may monitor your use of computers, tablets and emails**
- **You will ask for help and advice from a member of staff if you are not sure about any website you wish to use or if you feel you have done something wrong**
- **You will be polite and use language appropriately when you communicate online**
- **You will report any concerns you have about anyone being bullied or pressured online**
- **You will understand that if you do not comply with this acceptable use policy you may have the privilege of network use withdrawn and be subject to disciplinary procedures**

Appendix 2: Acceptable Use of ICT for Staff

Policy for the Acceptable Use of ICT - May 2019

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

- Report any accidental damage immediately to ICT Support
- Have due regard to, and comply with, the school'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 at Ninestiles or during any periods of extended leave, eg maternity/paternity 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 kept securely at all times, in the classroom, around school, during transit and at home and accept that the cost of any avoidable accidental damage may be charged back to my faculty
- Take responsibility for any personal use by members of my family to ensure that it is appropriate and within the letter and spirit of school policies
- Take good care of the device

Policy for the Acceptable Use of email and the Internet May 2019

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 schools. All of 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 schools 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 school, as well as the potential costs of time wasting, that can be avoided by following the practices outlined.

Although any staff devices are provided first and foremost for business use, they may be used for personal use at appropriate times in an appropriate manner. At all times users should take into account these guidelines and adhere to them.

1.2 Scope

These guidelines apply to all members of staff who have access to e-mail or the Internet.

1.3 Publicising the guidelines

Effective communication is vital to increase staff awareness of these guidelines and their use within Summit Learning Trust schools. 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 in the staff shared area.

New starters should not be given access to e-mail or the Internet until they have seen and accepted these policies. This will be the responsibility of their line manager.

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 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 sexually explicit material.

Although Summit Learning Trust respects the privacy of every individual throughout the organisation, all external mail (both incoming and outgoing) will be checked for content and attachments to make sure that at all times the security and integrity of the 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 any users who are found to breach the policies outlined in these guidelines. Significant abuse, particularly involving access to pornographic or offensive images constitutes gross misconduct and may lead to dismissal.

PART 2 – RESPONSIBILITIES

2.1 LGB (Local Governing Body)

The policies and these guidelines have been approved and adopted by the 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 Learning Trust ICT Department

Through the use of the filtering software, the Trust ICT department will monitor Internet and e-mail use and the subsequent analysis of this data (in accordance with the Internet and E-mail Analysis procedure). Also, the appropriate security virus prevention mechanisms will be maintained and updated to meet the ongoing requirement of all schools.

2.4 Members of Staff

All staff, with access to e-mail and the Internet will be held responsible for complying fully with the school computer policies and guidelines.

PART 3 - E-MAIL GUIDELINES

3.1 Personal Use

Members of staff are permitted to send personal e-mails as long as this does not interfere with their job responsibilities. It should be noted that e-mail messages are not guaranteed to be private and all remain the property of the school and Trust.

3.2 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 that is viewed as highly confidential or valuable to the school 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 if necessary 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 can monitor, review and record all e-mail usage, and these will be used.

Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to his or her e-mail.

3.3 Etiquette

At all times users should use appropriate etiquette when writing emails (an email protocol to follow).

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.

3.4 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 school Equal Opportunities Policy.

3.5 Virus Protection

To prevent the risk of potential viruses, users should not open any unsolicited email attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus, they need to contact the Ninestiles ICT Help Desk immediately and close the message and attachment. It should not be accessed again without approval from the Network Manager.

In some instances, it might be appropriate to inform the original sender that their message contained a virus. Advice should be sought from ICT.

3.6 Security

Email is an effective way of communicating confidential information. This is only the case, however, if passwords are secure. To maintain security it is good practice for users to keep their passwords confidential to themselves.

E-mail should not be left running unattended in any circumstances where this may lead to unauthorised access. The system should be closed and reopened on return. In no instances should a user login using a colleague's password unless permission has been given.

Where access to a mailbox is required, ICT can set up temporary passwords. Prior permission must be received from the individual concerned or their senior manager.

3.7 Housekeeping

Emails and attachment's should be deleted regularly or, if necessary, archived to a separate folder.

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 in particular if they are large files. Guidance is available from the ICT Support team.

PART 4 - INTERNET GUIDELINES

4.1 Rules for business use

All users will be provided with access to the internet.

Members of staff should not download any material that is not directly related to their job responsibility. This especially relates to screensavers, images, videos games, music files etc.

ICT should be notified before any software is downloaded for business use: all downloaded software needs to be properly licensed and registered. Any such software automatically becomes

the property of the Trust**.** There are systems in place to monitor all Internet usage including any software downloads.

If in doubt, please consult the ICT Support Team.

4.2 Personal use

Members of staff are permitted to access the Internet for personal use on a limited basis as long as this does not interfere with them carrying out their duties in an effective and efficient way. Members of Staff accessing the Internet for personal use are expected to be professional and reasonable. Excessive or regular use of the Internet for personal use during working hours, without any attempt to make up the time, would be considered to be failing in one's duties and could be subject to disciplinary action under the School's Disciplinary Policy.

It should be noted that there are systems in place that can monitor and record all Internet usage, and these will be used. No user should have any expectation of privacy as to his or her Internet usage. Analysis of this information may be issued to the Principal, if required.

4.3 Respecting copyright

Employees 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.

4.4 Security

Systems are in place to protect the school and Trust information systems. However users must also be aware of the potential risks associated with accessing the Internet. Employees are reminded that newsgroups are public forums where it may be inappropriate to reveal confidential information.

Also, see section 4.2 above.

Users are also reminded that unauthorised usage of a computers could include accessing email or the Internet via a computer other than your own even if doing so under your own user identification.

4.5 Virus protection

Although virus protection software is installed on all networked computers, users should be aware of the potential hazards associated with computer viruses. Any files that are downloaded will be scanned for viruses before being accessed. If you have any concerns about viruses on the Internet or think you may have accessed material that contains a virus please contact the ICT Help Desk.

4.6 Inappropriate websites

Under no circumstances should a user access a site that contains sexually explicit or offensive material. If you find yourself connected to such a site inadvertently, you should disconnect from that site immediately, and notify your line manager.

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

Appendix 3: online safety training needs – self-audit for staff

Adapt this audit form to suit your needs.

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in School?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the School's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the School's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the School's ICT systems?	
Are you familiar with the School's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**