



Date of review: September 2019

Next review: September 2021

Responsible person: Assistant Principal [Student Welfare]

Online Safety Policy

Contents

1. Aims.....	2
2. Legislation and guidance.....	2
3. Roles and responsibilities.....	2
4. Educating Students about online safety	4
5. Educating parents about online safety	5
6. Cyber-bullying	5
7. Acceptable use of the internet in Academy.....	6
8. Students using mobile devices in Academy.....	6
9. Staff using work devices outside Academy.....	7
10. How the Academy will respond to issues of misuse.....	7
11. Training	7
12. Monitoring arrangements.....	8
13. Links with other policies	8
Appendix 1: acceptable use agreement (Students and parents/carers).....	9
Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors)	11
Appendix 3: online safety training needs – self-audit for staff	12
Appendix 4: online safety incident report log	13

.....

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of Students, staff, volunteers and Trustees
- 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

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 Academy's 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 Students' 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 Trustees

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

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

All 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 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 Academy.

3.3 The Designated Safeguarding Lead (DSL)

Details of the Academy's designated safeguarding lead (DSL) Mr Ben Stevens are set out in our child protection and safeguarding policy.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- 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 Academy 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 Academy to the Principal and/or Trustees

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep Students safe from potentially harmful and inappropriate content and contact online while at Academy, including terrorist and extremist material
- Ensuring that the 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 the Academy's ICT systems on a monthly 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 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 Academy behaviour policy

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 Academy's ICT systems and the internet (appendix 2), and ensuring that Students follow the Academy'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 Academy 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 Academy's ICT systems and internet (appendix 1)

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 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 2).

4. Educating Students about online safety

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

In **KEY STAGE 3**, Students 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

Students 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.

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

5. Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, 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/CPC.

Any specific concerns will be discussed with parent/carer on an individual basis

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 Academy behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

The Academy will actively discuss cyber-bullying with Students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies where appropriate.

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

The Academy will send 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 Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among Students, the Academy will use all reasonable endeavours to ensure the incident is contained.

The DSL/CPC will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Academy 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 Students' 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 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 Academy discipline), and/or
- Report it to the police

Any searching of Students 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 Students' electronic devices will be dealt with through the Academy complaints procedure.

7. Acceptable use of the internet in Academy

All Students, parents, staff, volunteers and Trustees are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

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.

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

Any inappropriate use will be dealt with in accordance with safeguarding & CP policy and the behaviour policy.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in Academy

Students may bring mobile devices to the Academy, but are not permitted to use them when inside the Academy grounds during:

- Lessons
- Breaks
- Tutor group time
- Clubs before or after the school day, or any other activities organised by the Academy

Any use of mobile devices in Academy by Students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the Academy behaviour policy, which may result in the confiscation of their device. Devices will need to be collected by the student at the end of the day or by parents if the student continues to break the Academy rules. This will allow SLT the opportunity to discuss the issues pertaining to mobile device use within the Academy.

9. Staff using work devices outside Academy

Staff members using a work device outside of the Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix 2.

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 of the Academy. Any USB devices containing data relating to the Academy must be encrypted.

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

Work devices must be used solely for work activities.

10. How the Academy will respond to issues of misuse

Where a student 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 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. 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 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 CPCs 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 about online safety at regular intervals, and at least annually.

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/CPCs logs behaviour and safeguarding issues related to online safety via CPOMS. An incident report log can be found in appendix 4. This will be logged and followed up in accordance with the Safeguarding & CP policy.

This policy will be reviewed biannually by the Principal. At every review, the policy will be shared with the Trustees.

13. Links with other policies

This online safety policy is linked to our:

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

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

Acceptable use of the Academy's ICT systems and internet: agreement for Students and parents/carers

Name of student:

When using the Academy's ICT systems and accessing the internet in Academy, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- 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
- Share my password with others or log in to the Academy's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- 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 Academy:

- I will not use it during the Academy grounds without a teacher's permission
- I will not use it within the Academy building, unless directed by a member of staff
- 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.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the Academy's ICT systems and internet responsibly.

Signed (student):

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 Students using the Academy's ICT systems and internet, and for using personal electronic devices in Academy, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors)

Acceptable use of the Academy's ICT systems and the internet: agreement for staff, Trustees, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the Academy's ICT systems and accessing the internet in Academy, or outside Academy on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- 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
- Share my password with others or log in to the Academy's network using someone else's details

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.

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 student 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 Students in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

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

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 Academy?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the Academy’s acceptable use agreement for staff, volunteers, Trustees and visitors?	
Are you familiar with the Academy’s acceptable use agreement for Students and parents?	
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?	
<p>Are there any areas of online safety in which you would like training/further training? Please record them here.</p>	

Appendix 4: online safety incident report log

Incident	<input type="text"/>
Categories	<input type="checkbox"/> Behaviour Related Log <input type="checkbox"/> Bullying/ Friendship Related Issues <input type="checkbox"/> Cause for Concern <input type="checkbox"/> Child Protection <input type="checkbox"/> Contact with External Agency <input type="checkbox"/> Home Issues/ Parenting Issues <input type="checkbox"/> Medical Issues <input type="checkbox"/> Parental Contact <input type="checkbox"/> Safeguarding <input type="checkbox"/> SEND <input type="checkbox"/> Team Teach Incident <input type="checkbox"/> Verbal & Aggressive Incidents
Linked student(s)	<input type="text" value="Begin typing a student's name"/> Type a student's name to link them to this incident.
Body map	<input type="text"/>
Date/Time	<input type="text" value="Thu 20 June 2019"/> <input type="text" value="4:57PM"/>