Online Safety Policy

Written by:	Janine Dix	**Date:**	June 2021
Last reviewed on by:	11/02/23		
Next review due by:	11/02/2025		
Approved by:	LGB		
Version:	3		

1 Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers 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

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 also incorporates Derbyshire guidance from their briefing note in June 22 about online challenges and hoaxes.
DDSCP Briefing Note Harmful Online Challenges and Hoaxes June 2022.pdf (proceduresonline.com)

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.

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 Local Governing Board

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body 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 governors 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 Headteacher

The Headteacher 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) are set out in our child protection and safeguarding policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the Headteacher, 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 the academy to the Headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager for Esteem MAT 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 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

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 ICT systems and the internet (appendix 2), and ensuring that pupils follow the academy's terms on acceptable use (appendix 1)
- Working with the DSLs 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 Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (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 pupils about online safety

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

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.

The academy will use tutor-based activities, one to one lessons and effective use of the curriculum 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

The academy 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, induction meetings and parent placement review meetings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSLs.
Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

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 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 academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class groups, tutor-based activities, one to one lessons and effective use of the curriculum the issue will be addressed in.

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, Governing Body members 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 academy 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 academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained. The DSL 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 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 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

A staff member alone should not delete online material on a pupil's device. 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 academy complaints procedure.

7 Online Challenges and Hoaxes (DDSCP briefing Guidance June 22)

What are online challenges and hoaxes?
Online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. A hoax is a deliberate lie designed to seem truthful.

Key considerations for all agencies working with children and their families
The agency's Safeguarding or Child Protection Lead should be involved in any pre-planning and decision making around any challenge or hoax. In most cases the Safeguarding or Child Protection Lead is likely to be best placed to lead

Online challenges and hoaxes can create considerable panic creating pressures to take immediate action. In all cases it is important to take a step back and undertake a case-by-case risk assessment:
• Consider the scale and nature of the possible risk to children and young people.
• Seek support and check the factual basis of any harmful online challenge or online hoax. You can do this via the UK Safer Internet Centre Professional Online Safety Helpline telephone 0344 381 4772 or helpline@saferinternet.org.uk.
Having an agreed agency plan in place for responding to online challenges and online hoaxes can be really helpful as they support a more measured and effective approach to any concerns when they arise. Plans can be outlined within online safety policies and include letting staff know about who to go to if they have concerns about an online challenge or hoax. Agencies should also consider letting children and young people, parents, carers and staff know in advance, about what they are likely to do when a harmful online challenge or online hoax begins to circulate.

Supporting and protecting children and young people

All agencies and staff should:

✓ Provide safe spaces for children and young people to talk about their online life and to ask questions and share concerns about what they experience online or elsewhere.

✓ Ensure there are well promoted, easily understood and easily accessible systems in place for children and young people to confidently report any worries, concerns or abuse.

✓ Consider how best they can support children and young people to learn about online safety, in a way that is appropriate for their age and stage of development.

✓ Ensure they have appropriate online filters and monitoring systems in place.

✓ Share helpful online safety messages with parents and carers, including practical advice about talking to children about their online lives, responsible use, enabling privacy settings, setting parental controls, blocking, reporting and support services.

✓ Consider if a child or young person needs additional support, including via an early help assessment and where there are child protection concerns, a referral to children's social care.

✓ Follow agency safeguarding/child protection policies and refer to the DDSCP multi-agency safeguarding children procedures.

Alert relevant authorities

Following advice from the UK Safer Internet Centre Professional Online Safety Helpline about your concern or evidence an online challenges or hoax has the potential to harm children and young people, key local agencies must be informed. The DDSCP Safeguarding Children Procedures include a list of all local contact details.

Helpful resources

• Harmful online challenges and online hoaxes guidance (DfE) to help settings prepare for and deal with any harmful online challenge or online hoax which might be circulating between children and young people.
• Advice for schools on responding to online challenges (UK Safer Internet Centre)
• De-escalating and responding to harmful online challenges (UK Safer Internet Centre)
• Video - Responding to Online Challenges - Advice from the Professionals Online Safety Helpline (POSH) (UK Safer Internet Centre)
• Parents – scare or prepare? (LGfL) – blog with links to 'scary online challenges' poster and video for professionals
• Think before you scare (The Education People)
• There's a viral scare online. What should I do? (ThinkuKnow) - advice for parents and carers
• Exploring critical thinking online (UK Safer Internet Centre)
• Education for a Connected World (UK Safer Internet Centre) describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives.
• Project Evolve – resources, activities and professional development materials supporting the Education for a Connected World framework

8 Acceptable use of the internet in academy sites

All pupils, parents, staff, volunteers and governors 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 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 in appendices 1 and 2.

9 Pupils using mobile devices in academy sites

Pupils hand in mobile phones and personal belongings at the start of their day. Pupils then receive personal items back when they are leaving the site. At KS3/4, at the discretion of site staff, pupils may have their mobile devices returned to them for a short period with monitored use to call a parent.

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

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

10 Staff using work devices outside of the academy

Staff members using a work device outside of a site building 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 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.

11 How the academy will respond to issues of misuse

Where a pupil 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.

12 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 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 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.

13 Monitoring arrangements

The DSL and deputies will log behaviour and safeguarding issues related to online safety. An incident report log can be found in my concern online safeguarding system if safeguarding is breached or a site incident form.

This policy will be reviewed every 2 years by a member of the SLT and approved by the Local Governing Body.

14 Links with other policies

This online safety policy is linked to our:

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

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

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

Name of Pupil:

When using the academy's ICT systems and accessing the internet 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 site:

- I will hand it in and it will be secured in a safe place
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission

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 (pupil):	Date:

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

Signed (parent/carer):	Date:

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteer and Visitors)

Acceptable use of the academy's ICT systems and internet: agreement for staff, Governors, volunteer and visitors

Name of Staff/Governor/Volunteer/Visitor:

When using the academy's ICT systems and accessing the internet on site, or outside the 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 network using someone else's details

I will only use the academy's ICT systems and access the internet on site, or outside the academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the academy will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding leads (DSLs) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the academy's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed:	Date:

Appendix 3: Online Safety Training Needs – Self-Audit for Staff

Online Safety Training Needs Audit	
Name of Staff/Governor/Volunteer/Visitor:	Date:
Do you know the name of the person who has lead responsibility for online safety at our academy?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for pupils 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?	
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