Shaw Education Trust

Online Safety Policy (e-safety)

Document Owner:	B Duffy
Approved By:	C-Suite
Queries to:	B Duffy
Review Period:	3 years
Last Review date:	1st September 2025

Section	Contents
1	Aims
2	Introduction
3	Responsibilities
4	Legislation & Guidance
5	Filtering & Monitoring
6	Social Media
7	Teaching Online Safety
8	Use of iPads across our Trust
9	Staff Training
10	Online safety at home – advice for parents/carers
11	Responding to concerns
12	The Use of Artificial Intelligence (AI) systems in schools
13	Information and Support

1. Aims

This policy applies to all staff, volunteers and pupils and anyone involved in our academy's activities. Its purpose is to:

- ensure the safety and wellbeing of our pupils is paramount when adults or pupils are using the internet, social media or mobile devices,
- provide staff and volunteers with the overarching principles that guide our approach to online safety,
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

It sits alongside and should be read in conjunction with all our Safeguarding Policies, including, Safeguarding and Child Protection Policy, Online Filtering & Monitoring Policy, Prevent Policy which protects children from radicalisation, and Use of Artificial Intelligence (AI) Policy. In addition, academies will have local policies which will in art address online safety and procedures, e.g. Behaviour Policy, Anti-Bullying procedures, etc.

2. Introduction

Being online is an integral part of children and young people's lives. The internet and online technology provide new opportunities for pupil learning and growth, but it can also expose them to many forms of risk. The use of technology has become a significant component of many safeguarding issues, e.g. child sexual exploitation, radicalisation, sexual predation, 'cyber'-bullying.

An effective approach to online safety empowers us, and parents/carers, to protect and educate our young people, and establish mechanisms to identify, intervene in, and escalate any incident where appropriate. More importantly, educating and empowering young people from an early age, building resilience and skills against online vulnerability, is more effective than monitoring and filtering later on.

The breadth of issues classified within online safety in terms of types of risk, mechanisms for educating, and systems for support, is quite considerable and our leaders in our academy use resources beyond the scope of this policy. Therefore, this policy cannot cover all aspects of online safety but endeavours to outline our guiding principles of educating and supporting our pupils against online vulnerabilities.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: 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:** online behaviour that increases the likelihood of, or causes, harm; for example, 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 scams. If you feel your pupils, pupils or staff are at risk, please report it to the Anti-Phishing Working Group

Online safety falls into our normal safeguarding procedures of reporting concerns and supporting pupils in dealing with any issue which may harm them or affect their well-being in any way. All staff at our academy take this responsibility seriously and we have adopted a 'whole-school' approach to online safety.

3. Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, some roles warrant specific responsibilities, as outlined very briefly below:

Headteacher and senior leaders should:

- ensure the safety (including online safety) of members of the school community, as defined in Keeping Children Safe in Education.
- be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- ensure that relevant staff carry out their responsibilities effectively and receive suitable training.
- ensure the school curriculum includes the teaching of an online safety education programme.

Trustees/Academy Councillors should:

- ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety

Designated Safety Lead (DSL) should:

- take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

All academy staff should:

- have an awareness of school Online Safety Policy and practices, including reporting systems.
- have read, and signed the staff acceptable use agreement (AUP).
- follow all relevant guidance and legislation including, KCSiE and UK GDPR regulations.
- ensure all digital communications with learners, parents and carers and others are on a professional level.
- supervise and monitor the use of all digital technologies during the course of their work.
- ensure there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.

Parents and carers should: (see also 'Online Safety' section below)

- reinforce the online safety messages to their children.
- monitor their child's internet use as appropriate.

Pupils should:

- take responsibility for their own and each other's' safe and responsible use of technology.
- ensure they respect the feelings, rights and values of other pupils in their use of technology at school and at home.

- understand how to report concerns they may have.
- know, understand and follow school policies on the use of technology.
- not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

4. Legislation & Guidance

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England and has been written in consultation and reference to many sources of good practice and guidance such as;

Keeping Children Safe in Education

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK.

Online Safety Act 2023

Teaching online safety in schools - GOV.UK

(See 'Information and Support' section for further documentation).

5. Filtering and Monitoring

The Department for Education's statutory guidance Keeping Children Safe in Education states that "it is essential that children are safeguarded from potentially harmful and inappropriate online material." As such, governing bodies and proprietors ensure appropriate filters and appropriate monitoring systems are in place in line with DfE standards. However, we also must ensure that over blocking does not lead to unreasonable restrictions as to what our pupils can be taught with regards to online teaching and safeguarding.

We have in place strict and high-level standards in this aspect of safeguarding which is regularly checked and reported on and in line with guidance and requirement of all schools. It is important to recognise however, that no filtering systems can be 100% effective and needs to be supported with good teaching and learning practice and effective supervision.

Where appropriate, pupils are issued with passwords to access our IT systems in school and are instructed to keep this confidential. We also have rules on the use of mobile devices in our academy which all pupils have to follow. As well as the disruption to teaching and learning, these rules are in place to safeguard pupils against possible online issues, at least while in our academy. Staff sign an 'Acceptable Use Policy' which covers staff use of technologies both inside and outside school.

6. Social Media

Whilst the internet is used by pupils for education purposes, away from lessons and school, most engage in some form of social networking, i.e. "the use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own". Apps such as WhatsApp, Tik-Tok, Instagram and Snapchat are of common use to young people. All of these have age restrictions, e.g. WhatsApp 16yrs and most others 13yrs, but in reality, many pupils under this age unfortunately access these online systems, which can make them vulnerable to grooming, cyber-bullying, radicalisation and other dangers.

Whilst pupils can be vulnerable to the approaches of others, i.e. 'contact', and what they see, i.e. 'content', it is in the risk area of 'conduct' where most issues arise in interaction with others. Behaviours such as posting and sharing inappropriate images of themselves and/or others including 'sexting' and commenting negatively on others can cause issues for pupils.

7. Teaching Online Safety

Alongside ensuring our online safety arrangements are robust, it's essential that we teach pupils about staying safe online.

We speak to our pupils about the benefits and dangers of the internet and create an open environment for pupils to ask questions and raise any concerns. We continually work to embed key messages about staying safe online throughout our curriculum and ensure that pupils in all year groups are taught online safety skills. As with all aspects of our whole-school curriculum, our 'online-safety teaching curriculum' is differentiated for all our pupils at an appropriate level to ensure they understand how to keep themselves safe online.

Areas such as radicalisation, grooming and bullying are covered in line with relevant policies including how each of these dangers can be increased through online activity. Pupils are educated on how to not only protect themselves from online dangers, but also to ensure that they themselves do not become active in any negative online behaviours such as cyber- bullying which can affect others.

We deliver our online safety ‘curriculum’ in a variety of methods across our academy, such as:

- In lessons where internet use is pre-planned, including IT/Computing lessons
- Where pupils are allowed to freely search the internet, e.g., using search engines
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of the study.
- In PSHE/SMSC curriculum/lessons
- Assemblies and guest speakers

8. Use of iPads

Many of our pupils across our Trust have access to school iPads. We have been diligent to ensure that our view of online safety extends to the use of iPads both inside our academies, and also at home, where relevant. A robust filtering and monitoring system is in place so that all our pupils’ safety is also monitored when iPads are used at home. Pupils have been taught how to use their iPads for use both at school and home.

9. Staff Training

All our staff undergo safeguarding training at regular intervals as well as at induction. Included in this training is online safety. This training is delivered in a variety of methods including in- school activities, attendance to external training, and of course participation in online training.

Our Designated Safeguarding Lead directs this training alongside other members of our Senior Leadership Team to ensure we have full coverage. Our Academy Council (Governors) also engage in safeguarding training, and we are supported by The Shaw Education Trust specialist leads in safeguarding.

In addition, our staff are governed by our 'Acceptable Use Policy' which covers their own use of internet and ICT facilities for work purposes but also gives advice and guidance on personal use of the internet, e.g. Social Networking sites, which will safeguard staff and ensure neither staff nor pupils are placed in vulnerable positions.

10. Online Safety at home – advice for parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Some parents/carers may themselves not fully understand the issues and are less experienced in the use of ICT than their child. We will endeavour to support our parents/carers where we can by signposting resources where necessary and ensuring we have a comprehensive curriculum and actions in place to help. In addition, school events such as parents' evenings etc. are used to offer more advice and guidance. Specific sessions on online safety can also be available when relevant. Our use of iPads means that many pupils across our trust can use their school iPad at home. Parents have been given advice and support around this.

In today's world access to the internet is extremely easy and many pupils, especially in secondary schools, have their own mobile phones. This makes the monitoring of internet use quite difficult for parents/carers which is why educating pupils on the dangers is always our priority. However, there are some steps parents/carers can take, *which may be age dependent*, such as:

- Educate themselves about social media
- Discuss with their child the dangers and consequences of social media
- Maintain an open dialogue with their child
- Set guidelines and rules with their child when first allowed to use social media
- Establish age limits for their child
- Explain the importance of privacy settings with their child and check them if relevant
- Keep the computer in a common area of the house
- Encourage them to never accept a 'friend's request' from people they don't know
- Explain importance of keeping passwords safe
- Encourage them to think before they post anything in an emotional reaction to something they have seen online

Lots of advice and guidance is available online for parents/carers. (see section 12 below).

11. Responding to concerns

Responding to concerns in this area fall into line with our normal safeguarding reporting procedures. When any staff becomes concerned regarding any issue, they report to our DSL and/or a member of our Senior Leadership Team dependent on immediate availability. An assessment of the risk is then made and appropriate actions taken.

If it is concerning content/activities which are deemed illegal, then we report to the police. If it is concerning material which has bypassed our filtering system, we ensure we block any further similar material coming from the same source. In addition, dependent on actions of any pupils, we deal with any disregard of our behaviour rules in our normal way using our behaviour and discipline polices, ensuring all the time that we continue and support the development of all our pupils.

12. The Use of Artificial Intelligence (AI) systems in schools

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving.

AI must be used safely across the trust to prevent harm, it is therefore important that staff and pupils understand the potential risks associated with AI-generated content, including misinformation, impersonation, and explicit or offensive material. The trust has therefore, created an AI Policy to cover all educational, operational and safeguarding principles of using AI appropriately and safely.

Some of the actions which will look to prevent AI-Generated Harm

- AI must not be used to create or share harmful, misleading, or inappropriate content
- Staff and pupils will receive regular and appropriate training to recognise and respond to AI risks such as deepfakes, misinformation, and impersonation
- The Trust's/schools filtering and monitoring systems will be maintained to detect and prevent AI-generated threats, (as per the Government's Filtering and Monitoring standards). The appropriate filtering and monitoring systems will attempt to block internet access to harmful sites and inappropriate content, including the detection of harmful AI material

- Any misuse of AI that poses a safeguarding concern will be addressed through the Trusts/school's safeguarding procedures

As AI systems become more integrated into our operations, cybersecurity risks must be managed to prevent unauthorised access, phishing attempts, and data breaches.

AI-related cybersecurity threats must be monitored and reported. The IT team will ensure that AI tools used across the trust do not introduce security vulnerabilities or compromise data protection.

13. Information and Support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The table below lists some links to relevant sites and their main purpose.

SCHOOL USE	
Organisation/Resource	What it does/provides
Plan technology for your school - GOV.UK	Find out how your school can plan and use digital technology better.
Online Safety for Schools | SWGfL	Includes a template for setting out online safety policies
PSHE Association | Charity and membership body for PSHE education	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
The use of social media for online radicalisation - GOV.UK	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCIS	The UK Council for Internet Safety's website provides: Sexting advice / Online safety: Questions for Governing Bodies / Education for a connected world framework
Education for a Connected World	A framework to equip children and young people for digital life
PARENTAL SUPPORT	

Organisation/Resource	What it does/provides
Ofcom's Children's Media literacy report 2024	Research on online use by children
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
SCHOOL AND HOME	
Organisation/Resource	What it does/provides
CEOP Education	NCA CEOPs advice on online safety
Resources | Childnet	Guidance for schools and parents on cyberbullying
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
NSPCC E-Safety for schools	Guidance and support for schools and parents
UK safer internet centre	Contains a specialist helpline for UK schools and colleges

Shaw Education Trust

Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
ST7 4DL

Twitter	@ShawEduTrust
LinkedIn	@ShawEducationTrust
Call	01782 948259
Email	info@shaw-education.org.uk
Visit	shaw-education.org.uk

Pupil & people centred

Act with integrity

Be innovative

Be best in class

Be accountable