Online eSafety & Information Security Policy

Providing Guidance to Support Students and Staff

Pine Green and Evergreen Academies

Current Author:	S. Williams
Person Responsible for the Policy:	D. Hartley

Last Review:	June 2025
Reviewed by:	Academy Council - Daniel Hartley
Date of Next Review:	June 2027

Contents Page

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 our; Prevent Policy which protects children from radicalisation, Anti-Bullying Policy, Online Monitoring and Filtering Policy, and of course our Safeguarding and Child Protection Policy.

Introduction

Being online is an integral part of children and young people's lives. The internet and online technology provides 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 establishes 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 (what a child can see and receive online): being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views,
- contact (when contact has been made with a child online): being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults,
- conduct (when a child interacts online by posting or uploading information): personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying,
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing 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.

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, NSPCC E-Safety for schools, UK Safer Internet Centre Online Safety Policy and DfE Teaching Online Safety. (See 'Information and Support' section for further documentation). The policy also has due regard to

- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

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 should ensure appropriate filters and appropriate monitoring systems are in place. However, we also have to 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.

Social Networking

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 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.

Teaching Online Safety

Alongside ensuring our online safety arrangements are robust, it's essential that we teach pupils about staying safe online DfE Teaching Online Safety in Schools, UK Council for Child Internet Safety.

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 students are allowed to freely search the internet, e.g., using search engines
- It is accepted that from time to time, for good educational reasons, students 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

Use of iPads

At time of publication of this policy, our trust has rolled out the use of iPads in many of our academies. 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 monitoring and filtering 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.

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 all 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.

E-Safety Control Measures

Internet access:

- All users in key stage 2 and above will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed on a regular basis and their activity is continuously monitored by the e-safety officer.
- The school has a monitoring and filtering system (Securly) which monitors internet usage..
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

Master users' passwords will be available to the headteacher for regular monitoring of activity.

- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

o Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy. o Staff are prohibited from using personal devices on the school networks.

Email:

- o Pupils and staff will be given approved email accounts and are only able to use these accounts.
- o The use of personal email accounts to send and receive personal data or information is prohibited.
- o No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- o Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- o Staff members are aware that their email messages are not monitored.
- o Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

Social networking:

- o Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- o Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- o Pupils are regularly educated on the implications of posting personal data online outside of the school.

o Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole. o Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

- o Staff are not permitted to publish comments about the school which may affect its reputability.

o Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

Mobile devices and hand-held computers:

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use, such as a pupil escalating in behaviour.
- Pupils or staff are not permitted to access the school's Wi-Fi system at any times using their personal mobile devices or personal hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises

Network Security

Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.

Passwords have a recommended minimum length of 7 characters and include one Upper Case and one Special character to prevent 'easy' passwords or mistakes when creating passwords.
Virus management:

Technical security features, such as virus software, are kept up-to-date and managed by the e-safety officer.

The e-safety officer will ensure that the filtering of websites and downloads is upto-date and monitored. 5.8.

Cyber Bullying

For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our safe guarding policy.

The headteacher will decide whether it is appropriate to notify the police or antisocial behaviour coordinator in their LA of the action taken against a pupil.

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. Many parents/carers can 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 are able to 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/cares 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 including from the UK Safer Internet Centre.

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.

Information and Support

There is a wealth of information available to support schools, colleges and parents to keep children safe online.

UKCIS has published its Education for a connected world framework, which aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed to be usable across the curriculum and beyond and to be central to a whole school approach to safeguarding and online safety. It covers early years through to age 18.

As well as those resources already noted in this policy, the following list, taken from KCSiE 2019, should provide a useful starting point for readers to extend knowledge and build up resources and advice:

Organisation/Resource	What it does/provides

thinkuknow	NCA CEOPs advice on online safety

UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
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
childnet	Guidance for schools and parents on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	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

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