Central Region Schools Trust

Founded by the RSA

ONLINE SAFETY POLICY

Recommended by:	COO in absence of Head of IT
Recommendation Date:	October 2021
Ratified by:	Audit Risk and Standards Committee
Signed:	
Position on the Board:	Chair of Audit Risk and Standards Committee
Ratification Date	2 November 2021
Next Review:	September 2022
Policy Tier (Central/Hub/School):	Central

Contents

1. Aims

Central Region Schools Trust 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 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.

3. Roles and responsibilities

Online safety depends on schools, staff, governors, parents and the pupils themselves taking responsibility for their actions online. Staff have a particular responsibility to supervise pupils, plan access and be an appropriate role model. The balance between educating pupils to take a responsible approach and the use of regulation must be judged carefully.

3.1 The local academy governing board

The governing board has overall responsibility for monitoring this policy and holding the principal/head of school to account for its implementation.

All governors will:

- ensure that they have read and understand this policy

3.2 The Principal/Head of School

The principal/head of school is responsible for:

- ensuring the safety of all members of the school community
- ensuring adequate CPD is provided on issues concerning online safety within the school
- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- following procedures in the event of a serious online safety allegation being made against or concerning a member of staff or pupils within the school

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy safeguarding lead/s are set out in our safeguarding children policy.

The DSL is responsible for:

- supporting the principal/head of school in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the principal/head of school, network manager and other staff, as necessary, to address any online safety issues or incidents

- having an up to date awareness of online safety matters
- annually reviewing the online safety policy of the school
- providing training within the school community on online safety
- logging all online safety incidents to help inform for future online safety practices/developments
- attending relevant professional development meetings where appropriate
- providing regular reports on online safety in school to the senior leadership team and/or governing board

This list is not intended to be exhaustive.

3.4 The network manager with oversight by the Head of IT

The network manager with oversight by the Head of IT 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- remaining at the forefront of online safety technical information and inform/update others as necessary
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying or cyber-crime are referred as appropriate so they may be dealt with in line with the school behaviour policy
- ensure the appropriate level of security protection procedures are in place, in order to safeguard systems, staff and learners. The effectiveness of these procedures will be reviewed periodically to keep up with evolving cyber-crime technologies.
- ensuring data is held securely in line with the General Data Protection Regulation (GDPR). This list is not intended to be exhaustive.
- Support and advise the DSL and senior management team on monitoring and filtering requirements.
- Ensure DSL and senior management are aware of changes to existing, or the introduction of new systems that may change access to pupil data or records particularly with the use of cloud-based platforms.

3.5 All staff and volunteers

All staff, including contractors and agency staff, trainees 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, and ensuring that pupils follow the school's terms on acceptable use
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying or cyber-crime are dealt with appropriately in line with the school behaviour policy
- ensuring all digital communication with pupils is on a professional level and carried out using only school systems

- Staff are permitted to use their own personal devices if they wish but only if all school systems they are accessing are password protected.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- notify a member of staff or the principal/head of school of any concerns or queries regarding this policy
- ensure their child understands the issues surrounding online safety
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems and/or internet will be made aware of this policy and the ICT acceptable use policy, when relevant, and expected to read and follow them.

3.8 Pupils

Pupils are responsible for:

- ensuring they use school ICT systems and internet appropriately following this online safety policy & the ICT acceptable use policy
- understanding how to report issues of abuse/misuse within the school and know how to do so
- knowing and following school policy on the use of mobile devices, digital cameras as well as the use of images appropriately
- understanding the importance of good online safety practice when using digital technology both in and out of school

4. Education about online safety

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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **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**: personal 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 pupils, students or staff are at risk, this should be reported to the Anti-Phishing Working Group (https://apwg.org/) via the Trust Head of IT

4.1 Educating pupils

The purpose of using technology in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance school management functions.

Pupils are encouraged to use technology within school and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own safety and security.

Pupils will be taught to:

- use technology safely and respectfully
- recognise acceptable and unacceptable behaviour
- report concerns about content, contact, conduct and commerce
- protect their online identity and privacy
- understand how changes in technology affect safety

Safe use of social media and internet will also be covered in other subjects where relevant. The school will use the curriculum and assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4.2 Educating parents

Parents will receive information regarding online safety through school newsletters or other communications home and in information via our website. This policy will also be available to parents on the website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the principal/head of school and/or DSL

5. Cyber-bullying

5.1 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 may involve an imbalance of power.

5.2 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 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.

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 consider local safeguarding procedures when deciding whether an 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.

5.3 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, 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

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.

6. Cyber-Crime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;

• denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above

The network manager and Trust Head of IT will ensure the appropriate level of security protection procedures are in place, in order to safeguard systems, staff and learners. The effectiveness of these procedures will be reviewed periodically to keep up with evolving cyber-crime technologies.

If there are concerns about a pupil in this area, the designated safeguarding lead (or a deputy), will follow local West Midlands safeguarding procedure and may consider referring into the Cyber Choices programme

7. Acceptable use of ICT systems and the internet in school

All pupils, staff, volunteers and governors are expected to read and abide by the ICT acceptable use policies. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

8. Use of mobile technologies (3G/4G/5G)

Many pupils have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children could, whilst at school, bully or sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. For these reasons, it is school policy that mobile devices are switched off and

put away when entering the school site. There may be exceptional circumstances where students are allowed to use their device under the supervision of a member of staff, e.g student support, Photography lessons etc.

9. Remote learning

Staff and students may be provided with school owned devices in order to deliver lessons or continue to learn online at home.

All school owned devices internet and application usage (whilst at home) is monitored and logged to ensure compliance with the ICT acceptable usage policy.

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 safeguarding training, as part of their induction, including safe internet use and online safeguarding issues including cyber-bullying, cyber-crime 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 designated safeguarding lead and deputy safeguarding lead/s 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 safeguarding children policy.

12. How to report an online safety incident

Follow the normal behaviour policies for incidents where there is a safeguarding issue by referring to the Designated Safeguarding Lead.

If unsure, or the incident is potentially more serious, refer to the Principal and/or the Whistleblowing Policy.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding children policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Complaints policy
- Whistleblowing policy