Central RSA Academies Trust

E-SAFETY POLICY

Recommended by:	Head of IT
Ratified by:	Audit Risk and Standards Committee
Signed by:	
Position on the Board:	Chair of Audit Risk & Standards
Ratification Date	17 March 2021
Next Review:	September 2021*
Policy Tier (Central/Hub/School):	Central

*Update will be required following publication of KCSIE September 2021

Contents

.....

1. Aims

Central RSA Academies 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

E-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 e-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 e-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 esafety issues or incidents
- having an up to date awareness of e-safety matters
- annually reviewing the e-safety policy of the school
- providing training within the school community on e-safety
- logging all e-safety incidents to help inform for future e-safety practices/developments
- attending relevant professional development meetings where appropriate
- providing regular reports on e-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 e-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 e-safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 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 e-safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying 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

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 e-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 e-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 e-safety practice when using digital technology both in and out of school

4. Education about online safety

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 and contact
- 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 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 e-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 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.

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. 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.

7. 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.

8. 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 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.

9. How to report an e-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.

10. Links with other policies

This e-safety policy is linked to our:

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