

Author	Bob Stacey	Target group	All employees, consultants and volunteers
Owner	CfBT Schools Trust	Next review due	September 2019
Issued	September 2018		

E-Safety Policy

Aims

CfBT Schools Trust (the Trust) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Local Governors across all our Trust schools.
- 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.

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.

The policy also takes into account the [National Curriculum computing programmes of study](#) and complies with our funding agreement and articles of association.

Roles and responsibilities

Local Governing Body

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

The Local Governing Body will coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Local Governors will:

- ensure that they have read and understand this policy
- agree and adhere to the Trust's Acceptable Use Agreement.

Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding Policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- 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 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 school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or LGB.

This list is not intended to be exhaustive.

ICT manager

The ICT manager for each school 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.
- Conducting a full security check and monitoring the school's ICT systems on a regular 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 and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are reported appropriately so that they can be dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the Acceptable Use Agreement which sets out 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 are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

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 Acceptable Use Agreement which sets out the terms of acceptable use of the Trust's ICT systems and internet.

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>

Visitors and members of the community

Visitors and members of the community who use the school'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.

Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

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. Each 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.

Educating parents about online safety

Each school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

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 DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyber-bullying

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. Further detail on bullying can be found in our Anti-Bullying Policy.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying specifically, 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.

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, Local Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school 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 school will follow the processes set out in the anti-bullying and behaviour policies.

Examining electronic devices

School staff have the specific power 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. Our Behaviour Policy sets out full detail on this power.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use Agreement

All pupils, parents, staff, volunteers and Local Governors are expected to sign the Trust Acceptable Use Agreement – an agreement regarding the acceptable use of the Trust's ICT systems and the internet. Visitors will be expected to read and agree to the terms on acceptable use if relevant.

Use of the school'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.

Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them during lessons unless express consent to this is given by the teacher for the purpose of the lesson.

Any use of mobile devices in school by pupils must be in line with the CST Acceptable Use Agreement.

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the Trust's terms of acceptable use.

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 school. Any USB devices containing data relating to the school 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.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in the Trust's 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 system 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.

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 will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Local 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Trust.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints procedure
- Acceptable Use Agreement
- Staff Code of Conduct