ON LINE SAFETY POLICY

Policy Type	
Adopted by	**Trustees**
Chair of the Trustees	**Rev Nigel Sinclair**
Date	**23.05.2019**
To be reviewed	**23.05.2021**

Aims:

Elevate Multi Academy Trust (Elevate) and its Academies aim to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers, governors and Trustees;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust 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.

This policy complies with the Funding Agreement and Articles of Association.

Links with other Trust Policies and Practices:

Elevate Acceptable Use of ICT policy
Elevate Data Protection policy
Elevate Bring Your Own Device policy
Elevate Information Security policy
Elevate Child Protection and Safeguarding policy
Elevate Behaviour policy
Elevate Searching screening and confiscation policy
Elevate Complaints policy
Elevate Lap top agreement

Roles and Responsibilities:

The Local Governing Body(LGB):

The LGB has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The Safeguarding link governor will hold regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2).

The Head Teacher:
References below to 'the Head teacher' therefore include the Executive Head teacher, Head teacher or acting Head teacher as appropriate.

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

The DSL:
Details of the Academy's DSL and DDSL are set out in Elevate Child Protection and Safeguarding policy.
The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy;
- Working with the Head Teacher and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 4) 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 Elevate's Behaviour policy;
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in the Academy to the Head teacher and/or LGB;
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material;
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Ensuring that a monthly full security check and monitoring is conducted on the Academy's ICT systems;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with Elevate's Behaviour policy.

This list is not intended to be exhaustive.

All Staff and Volunteers:
All staff, including contractors and agency staff, 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 Academy's ICT systems and the internet (appendix 2), and ensuring that children follow the Academy's terms on acceptable use (appendix 1);
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy;

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with Elevate's Behaviour policy.

This list is not intended to be exhaustive.

Parents:
Parents are expected to:
- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1);

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 Academy'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 (appendix 2).

Educating Children about Online Safety
Children will be taught about online safety as part of the curriculum.
In **Key Stage 1**, children 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.

In **Key Stage 2** children 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 contac.t

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

Educating Parents about Online Safety:
- The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via its website.
- 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 Head Teacher and/or the DSL;

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

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. (See also the school behaviour policy.)

Preventing and Addressing Cyber-Bullying:

To help prevent cyber-bullying, the Academy will ensure that children understand what it is and what to do if they become aware of it happening to them or others. They will ensure that children know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The Academy will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teacher's will discuss cyber-bullying with the children in their classroom, and the issue will be addressed in assemblies.

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

The Academy 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 Academy will follow the processes set out in Elevate's Behaviour policy. Where illegal, inappropriate or harmful material has been spread among children, the Academy 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.

Examining Electronic Devices:

Academy 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 children's 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 Academy 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 children 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 children's electronic devices will be dealt with through Elevate's Complaints procedure.

Acceptable Use of the Internet in the Academy:

- All children, parents, staff, volunteers, Trustees and governors are expected to sign an agreement regarding the acceptable use of the Academy' s ICT systems and the internet (appendices 1 and 2);
- Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant;
- Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role;
- The Academy will monitor the websites visited by children, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils Using Mobile Devices in the Academy: if applicable

Year 6 children may bring mobile devices into the Academy, but must hand them to the class teacher at the beginning of the day. The mobile device will be handed to the child at the end of the school day.
Any breach by a child may trigger disciplinary action in line with Elevate's Behaviour policy, which may result in the confiscation of their device.

Staff Using Work Devices Outside the Academy:

See Elevate Lap Top Agreement.

Staff members using a work device outside the Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix 2.

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 the Academy. 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 Head Teacher.

Work devices must be used solely for work activities.

How the Academy will Respond to Issues of Misuse:

- Where a child misuses the Academy's ICT systems or internet, the Academy will follow the procedures set out in Elevate'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 Academy'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 Academy 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 and DDSL 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 Elevate's Child Protection and Safeguarding policy.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.
An incident report log can be found in appendix 4.

Appendix 1: Acceptable Use Agreement (children and parents or carers)

Acceptable use of the school's ICT systems and internet: agreement for children and parents or carers	
Name of Child:	
When using the Academy's ICT systems and accessing the internet in the Academy, I will not: • Use them for a non-educational purpose; • Use them without a teacher being present, or without a teacher's permission; • Access any inappropriate websites; • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity); • Use chat rooms; • Open any attachments in emails, or follow any links in emails, without first checking with a teacher; • Use any inappropriate language when communicating online, including in emails; • Share my password with others or log in to the Academy's network using someone else's details; • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer; • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. If I bring a personal mobile phone or other personal electronic device into the Academy: • I will hand it to the class teacher at the beginning of the school day and collect it from the teacher at the ned of the school day; • I will not use the device at the Academy. I agree that the Academy will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the Academy's ICT systems and internet responsibly.	
Signed (child):	**Date:**
Parent or carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of the Academy staff. I agree to the conditions set out above for children using the Academy's ICT systems and internet, and for using personal electronic devices in the Academy, and will make sure my child understands these.	
Signed (parent or carer):	**Date:**

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the Academy's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the Academy's ICT systems and accessing the internet in the Academy, or outside the Academy on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature; • Use them in any way which could harm Elevate and the Academy's reputation; • Access social networking sites or chat rooms; • Use any improper language when communicating online, including in emails or other messaging services; • Install any unauthorised software; • Share my password with others or log in to the Academy's network using someone else's details	
• I will only use the Academy's ICT systems and access the internet in the Academy, or outside the Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role; • I agree that the Academy will monitor the websites I visit; • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Academy, and keep all data securely stored in accordance with this policy and Elevate's data protection policy; • I will let the DSL know if a child informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material; • I will always use the Academy's ICT systems and internet responsibly, and ensure that children in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Online Safety Training Needs – Self-Audit for Staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in the Academy?	
Do you know what you must do if a child approaches you with a concern or issue?	
Are you familiar with the Academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the Academy's acceptable use agreement for children and parents?	
Do you regularly change your password for accessing the Academy's ICT systems?	
Are you familiar with the Academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Online Safety Incident Report Log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**