ON LINE SAFETY POLICY

Version	Author	Dated	Status	Details
1	Compliance Officer	23.05.2019	Approved Trustees	To be reviewed 23.05.2021
2	Head of Governance & Safeguarding	07.02.2023	Approved Trustees	
3				

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 Elevate to protect and educate the whole Trust community in its use of technology, including mobile and smart technology, including SMART watches or any internet enabled personal devices (which are referred to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key Categories of Risk

Elevate's approach to online safety is based on addressing the following categories of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- **Contact**: being subjected to harmful online interaction with other users, such as 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, such as 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

Legislation and Guidance:

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

[Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE'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 children's' electronic devices where they believe there is a 'good reason' to do so.

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 and Anti Bullying policy
Elevate Searching Screening and Confiscation policy
Elevate Complaints policy
Elevate Lap Top agreement

Roles and Responsibilities:

Trustees

All Trustees:

- Will ensure that they have read and understand this policy;
- Will agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 3);
- Will ensure that online safety is a running and interrelated theme while monitoring and implementing a whole Trust approach to safeguarding and related policies and/or procedures;
- To delegate to the Local Governing Body:
  - To ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some children with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable;
  - To ensure their Academy has appropriate filters and monitoring systems in place;
  - To ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified;
  - To consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

The Local Governing Body(LGB):

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

The Safeguarding link governor will hold regular meetings with appropriate staff to discuss online safety, and monitor the information 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 3);

- Ensure that online safety is a running and interrelated theme with their approach to monitoring safeguarding;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some SEND children. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- To ensure their Academy has appropriate filters and monitoring systems in place;
- To ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified;
- To consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

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:
- Ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy;
- Working with staff to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with Elevate's Child Protection and Safeguarding policy;
- Ensuring that any online safety incidents are logged on CPOMs 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 Academy's Behaviour and Anti Bullying policy;
- Updating and delivering staff training on online safety and recording the training;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in the Academy to the LGB.

The ICT Providers

The ICT providers are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that Elevate's Academies 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 Academies ICT systems on a weekly basis;

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- 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 Elevate's Academies 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 Elevate's Academies ICT systems;

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 3), and ensuring that children follow the Academy's terms on acceptable use (Appendix 1 or 2);
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's Behaviour and Anti Bullying policy;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

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 or 2);

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 3).

Educating Children about Online Safety

Children will be taught about online safety as part of the curriculum.

All schools have to teach:

Relationships education and health education in primary schools.

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 contact.

By the **end of primary school**, children will know:

- That people sometimes behave differently online, including by pretending to be someone they are not;
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when they are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- How information and data is shared and used online;
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some SEND children.

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.
- The Academy will let parents know:
  - What systems the Academy uses to filter and monitor online use;
  - What their children are being asked to do online, including the sites they will be asked to access and who from the Academy (if anyone) their child will be interacting with online.

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 Academy's Behaviour and Anti Bullying 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, Trustees, 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 the Academy's Behaviour and Anti Bullying 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices:
The Head teacher, and any member of staff authorised to do so by the Head teacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or children, and/or
- Is identified in the Academy rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Any searching of children will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Elevate's Searching, Screening and Confiscation Policy

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image;
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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.

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.

Children 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 the Academy's Behaviour and Anti Bullying policy, which may result in the confiscation of their device.

Staff Using Work Devices Outside the Academy:

See Elevate Lap Top Agreement.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate Elevate's terms of acceptable use, as set out in Appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek IMMEDIATELY advice from the IT Provider.

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 THE Academy's Behaviour and Anti Bullying 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/staff code of conduct;
- 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);

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages;
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
  - Sharing of abusive images and pornography, to those who don't want to receive such content.

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse;
- Develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks;
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term.

- 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.

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

Acceptable use of the school's ICT systems and internet: EYFS KS1: Agreement for children and parents or carers

Name of Academy:

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.

When I use the Academy's ICT systems (like computers, IPads) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them;
- Only use websites that a teacher or adult has told me or allowed me to use ;
- Tell my teacher immediately if:
  - I click on a website by mistake;
  - I receive messages from people I do not know;
  - I find anything that may upset or harm me or my friends.
- Use The Academy's computers for school work only;
- Be kind to others and not upset or be rude to them;
- Look after the Academy's ICT equipment and tell a teacher straight away if something is broken or not working properly;
- Only use the username and password I have been given;
- Try my hardest to remember my username and password;
- Never share my password with anyone, including my friends;
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer;
- Save my work on the Academy network;
- Check with my teacher before I print anything;
- Log off or shut down a computer when I have finished using it.

I agree that the Academy will monitor the websites I visit and that there will be consequences if I do not follow the rules.

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 end of the school day;
- I will not use the device at the Academy.
- I agree that the Academy will monitor the websites I visit.

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: KS2, Acceptable Use Agreement (children and parents/carers)

Acceptable Use of The Academy's ICT Systems and Internet: Agreement for Children and Parents/Carers	
Name of Academy:	
Name of Child:	

I will read and follow the rules in the acceptable use agreement policy.

When I use the Academy's ICT systems (like computers and IPADs) and get onto the internet in school I will:

- Always use the Academy's ICT systems and the internet responsibly and for educational purposes only;
- Only use them when a teacher is present, or with a teacher's permission;
- Keep my usernames and passwords safe and not share these with others;
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others;
- Always log off or shut down a computer when I've finished working on it.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- 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;
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- Log in to the Academy's network using someone else's details;
- 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 school:

- I will hand it in at the beginning of the day to my class teacher and collect it from my class teacher at the end of the school day;
- I will not use it during lessons, tutor group time, clubs or other activities organised by the Academy.

I agree that the Academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (child):	**Date:**

Parent/carer's 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 school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use Agreement (staff, governors, Trustees, 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/Trustee/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 its Academies 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 Academies network using someone else's details; • Take photographs of children without checking with teachers first (staff only); • Share confidential information about the Academy, its children or staff, or other members of the community; • Access, modify or share data I am not authorised to access, modify or share; • Promote private businesses**.**	
• 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/Trustee/volunteer/visitor):	**Date:**