EMPOWER
LEARNING ACADEMY TRUST

Approved by Trust/Committee	**Aug 2026**
Publication Date	**September 2026**
Owner/Reviewer	**CEO**
To be reviewed:	**July 2027**
Location	**Website**
Impact assessed:	**Y**

ONLINE SAFETY POLICY

Contents

1. Aims 1
The 4 key categories of risk 1
2. Legislation and guidance 1
3. Roles and responsibilities 2
3.1 The Trust Board 2
3.2 The Headteacher 3
3.3 The Designated Safeguarding Lead (DSL) 3
3.4 The ICT manager 3
3.5 All staff and volunteers 4
3.6 Parents/carers 4
3.7 Visitors and members of the community 5
4. Educating pupils about online safety 5
4.1 Pupils will be taught about online safety as part of the curriculum 5
4.2 Pupils will be taught practical cyber security skills 7
5. Educating parents/carers about online safety 7
6. Cyber-bullying 8
6.1 Definition 8
6.2 Preventing and addressing cyber-bullying 8
6.3 Examining electronic devices 9
6.4 Artificial intelligence (AI) 10
7. Acceptable use of the internet in school 10
8. Appropriate filtering and monitoring 10
9. Communication systems 11
10. Cloud platforms and data 11
11. Digital images and video 12
11.1 Staff responsibilities 12
11.2 Taking and storing images 12
11.3 Ai and image abuse 12
12. Social media 13
12.1 Management 13
12.2 Platforms 14
13. Social media and community 14
13.1 Behaviour and complaints 14
13.2 Parental support 14
13.3 Boundaries 15
14. Academy websites 15
15. Pupils using mobile devices in school 16
16. How the Trust will respond to issues of misuse 16
17. Training for Staff, Governors and Volunteers 16
18. Monitoring arrangements 17
19. Links with other policies 18
Appendices 19
Appendix 1: Key online-safety staff 19

1. Aims

Empower Learning Academy Trust (ELAT) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

2. 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**
- **Meeting digital and technology standards**
- **Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff**
- **Relationships and sex education (RSE) and health 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 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 our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the headteachers to account for its implementation.

The Trust Board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Trust Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Trust Board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Trust Board will make sure that the academies teach pupils how to keep themselves and others safe, including online.

The Trust Board will make sure that the academies have appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the **DfE's filtering and monitoring standards**, and discuss with IT staff and service providers what needs to be done to support the academies in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the academies' safeguarding needs

All trustees and local governance board members will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academies' ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils 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

3.2 The Headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the academies' designated safeguarding leads (DSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and Trust Board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Trust's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged in MyConcern / CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the behaviour policy
- Updating and delivering staff training on online safety (appendix 4 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 to the headteacher and/or Trust Board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Making sure that the 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
- Making sure that any online safety incidents are logged in the schools safeguarding reporting system and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy

This list is not intended to be exhaustive.

3.5 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 Trust's ICT systems and the internet (appendix 3), and making sure that pupils follow the Trust's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by contacting the IT Helpdesk.
- Following the correct procedures by contacting the IT Helpdesk if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to make sure that any online safety incidents are logged in the schools safeguarding reporting system and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the Trust's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – **UK Safer Internet Centre**
- Help and advice for parents/carers – **Childnet**
- Parents and carers resource sheet – **Childnet**

3.7 Visitors and members of the community

Visitors and members of the community who use the Trust's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

- **Relationships education and health education** in primary schools
- **Relationships and sex education and health education** in secondary schools

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up

- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

In **KS3**, 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 **KS4** 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

By the **end of secondary school**, pupils will know:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught

where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong

- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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 pupils with SEND.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The Trust will raise parents'/carers' awareness of internet safety in letters and other communications home, and in information via our websites. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings/meetings.

The academies will let parents/carers know:

- What systems the Trust 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

If parents/carers 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.

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the behaviour policy.)

6.2 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 encourage them to do so, including where they are a witness rather than the victim.

The academies will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form tutors will discuss cyber-bullying with their classes/tutor groups, and it will be addressed further in assemblies and workshops.

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 pupils, as part of safeguarding training (see section 11 for more detail).

The Trust's academies also send information on cyber-bullying to parents/carers so 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 academies will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academies 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.

6.3 Examining electronic devices

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

- Poses a risk to staff or pupils, 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

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the Academy or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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 searching of pupils 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**
- Our behaviour policy

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

ELAT recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

ELAT will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign 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 Trust's's terms on acceptable use, if relevant.

Use of the internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

More information is set out in the acceptable use agreements. Staff, volunteers and governors are to sign the ELAT Acceptable Use Policy

8. Appropriate filtering and monitoring

ELAT academies use the internet connection provided by LGfL TRUSTnet. This means all academies have a dedicated, secure, school-safe connection that is protected with firewalls and multiple layers of security, including a base layer of web filtering system, which is made specifically to protect children in schools.

Smoothwall Filter is used at local level within each Academy, providing granular auditable internet access to staff and students. Both LGfL and Smoothwall Filtering are Certified UK Safer Internet Centre Appropriate Filtering solutions.

Appropriate Monitoring is provided by Smoothwall Monitor, installed on all Academy owned devices including; PC's, Laptops, iPads, Chromebooks.

Live monitoring is triaged by Smoothwall human review, with alerts raised by Telephone call or Email to the appropriate delegated safeguarding staff depending on severity. Automated alerts are tied into our Safeguarding reporting systems MyConcern / CPOMS.

All Devices provisioned for student home use are configured with Smoothwall Monitor and Smoothwall Cloud Filter to ensure students are safe whilst using school owned devices, these devices are also controlled by the Meraki MDM (Mobile Device Management) platform to ensure these systems remain tamper proof.

9. Communication systems

Empower Learning Academy Trust provides appropriate managed communications platforms for staff and student use. All Trust approved platforms are auditable and subject to appropriate monitoring and filtering.

General principles for email and messaging are as follows:

- Academy email systems and messaging within learning environments managed by academies are the only means of electronic communication to be used between staff and pupils or staff and parents (in both directions). Any unauthorised use of a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member). There should be no circumstances where a private email or messaging is used.
- Staff or pupil personal data should never be sent / shared / stored on email.
  - If data needs to be shared with external agencies, it should be sent encrypted using a password protected zip file. Internally, staff should use the academy's network, including when working from home, or an academy-managed platform, such as OneDrive/SharePoint.
- Appropriate behaviour is expected at all times, and the academy-managed systems should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the academy into disrepute or compromise the professionalism of staff.
- Staff are allowed to use the email and messaging system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their messages may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to inappropriate sites may be blocked and not arrive at their intended destination.

10. Cloud platforms and data

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- New cloud systems and what may or may not be stored in them are approved by the DSL / OSL in consultation with technical staff. This is noted in a DPIA (data-protection impact statement) and parental permission is sought in line with GDPR requirements
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and / or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images / videos are only made public with parental permission
- Only academy-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

11. Digital images and video

When a pupil joins one of our academies, parents / carers are asked if they give consent for their child's image to be used in photographs or videos for specific purposes. These uses are beyond 'legitimate interests' such as internal assessment, which does not require express consent.

11.1 Staff responsibilities

- Whenever a photo or video is taken, a relevant member of school staff will check the latest records of parental consent and approve use of images for the intended purpose.
- Information about children online must be minimised, so images in public facing materials - such as academy websites and blogs - must not typically have any name attached, including in the file name and metadata. If deemed necessary by the school, it is acceptable to include a first name **only** alongside images of pupils/students.

11.2 Taking and storing images

- All staff are governed by their contract of employment and the academy's acceptable use policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. With permission from a member of the senior leadership team, staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to academy activities, taken without secrecy and not in a one-to-one situation, and always moved to academy storage as soon as possible, after which they are deleted from personal devices or cloud services.
- Photos are stored on the academy's network in line with the retention schedule of the Data Protection Policy.

11.3 AI and image abuse

There is no technology available that can reliably stop a digital image being manipulated using AI and any image could be used as the starting point for a generative Ai image. There are, however, some measures we can take to discourage images of children being used in the most distressing ways.

- To minimise the chance of distressing deepfakes, staff must not post front-facing, full-body images of children to any online service, such as school websites or blogs.
- Portrait shots (head and shoulders) and group shots are preferred - where each child is lower resolution and not full body – these may be less useful in producing the most harmful deepfakes.
- Multiple high-resolution images of the same pupil / student should be avoided to prevent realistic deepfake images being generated.

11.4 Communicating best practice

- Parents are reminded at appropriate times - e.g. before school productions - about the importance of not sharing images taken in school.
- Pupils are taught to think about their online reputation and digital footprint, so all staff should be good adult role models by not oversharing.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences.
- Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name and metadata of the file), that reveals the identity of others and their location. They are taught about the need to keep their data secure and what to do if they are subject to bullying or abuse.

12. Social media

Academies manage and monitor their social media footprint carefully to know what is being said about them academy and to respond to criticism and praise in a fair, responsible manner.

12.1 Management

- All social media accounts that are used to communicate on behalf of the school should be documented and approved by the Headteacher. Staff responsible for the accounts must be declared. To help us maintain school accounts over time and deal promptly with any unforeseen issues, editing rights must be given to the relevant Headteacher and the Digital Engagement team.
- Responses to online comments that may be contentious in any way must be approved by the Headteacher/Principal and/or the Trust's CEO.
- Staff responsible for managing social media accounts follow the guidance in the LGfL / Safer Internet Centre online-reputation management.
- All images of children must have the correct photo permissions and information about individual children online must be minimised (see Digital images and Video)

12.2 Platforms

While no social media platform is perfect, some are known to provide safeguarding risks or to provide harmful deepfake tools. Where this is the case, use of the platform on behalf of the school is not permissible.

13. Social media and community

Social media (including apps, sites and games that allow sharing and interaction between users) is a fact of modern life. However, as stated in the acceptable use policies which all members of the academy community sign, we expect everybody to behave in a positive manner, engaging respectfully with the academy and each other on social media as they would face to face.

13.1 Behaviour and complaints

- Posts must remain positive. Nothing must be posted that could be perceived as bullying, aggressive, insulting, illegal or otherwise inappropriate, or which might bring the academy or the teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
- If parents have a concern about the academy's online presence, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the Trust's complaints procedure should be followed. Sharing complaints on social media is unhelpful and can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the academy, which is important for the pupils we serve.
- Staff are reminded that they are obliged not to bring the Trust or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the academy or its stakeholders on social media and be careful that their personal opinions are not attributed to the academy, Trust or local authority, bringing the academy into disrepute.

13.2 Parental support

- Many social media platforms have a minimum user age of 13, but the academies deal with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage underage use.
- Academies must strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils / students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will typically learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking to their children about the apps, sites and games they use, with whom and for how long.

13.3 Boundaries

- Pupils are not allowed to be 'friends' with or make a friend request to any member of staff, governors, volunteers and contractors or otherwise communicate via social media. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the academy.
- Staff must not follow public student accounts and pupils / students should not follow staff, governor, volunteer or contractor public accounts. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- The academies have official social media accounts and will respond to general enquiries but asks parents / carers not to use these channels to communicate about their children. Academy-managed email and messaging are the official electronic communication channels between parents and the academy, and between staff and pupils.

14. Academy websites

Academy websites are key public-facing information portals for the academy community (both existing and prospective stakeholders) with a key reputational value. The Headteacher / Principal and Governors have given overall responsibility for the day-to-day updating the content to trusted members of staff.

14.1 Statutory information

The DfE has determined information which must be available on all school websites. Schools must comply with the requirements outlined at: **https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-online**.

14.2 Copyright

Academies have the same duty as any person or organisation to respect and uphold copyright law (schools have been fined for copyright breaches). Material must only be used with clear permission.

14.3 Safeguarding

Where staff submit information for the website, they are asked to remember that where pupils' work, images or videos are published, their identities are protected and full names are not included in accompanying text, file names or metadata. (see Social Media)

14.4 Reputation

As role models, staff should ensure that information posted on school websites is of the highest quality to support positive school and Trust reputations. This includes modelling good spelling, grammar, presentation and attention to detail.

15. Pupils using mobile devices in school

Mobile phones are banned in ELAT academies. Pupils must follow the individual academies' policies on use of mobile devices in school.

16. How the Trust 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 our policies on behaviour and acceptable use. 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 Trust'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 and the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Trust will consider incidents that involve potential illegal activity or content, or otherwise serious incidents, should be reported to the police.

17. Training for Staff, Governors and Volunteers

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, threatening, 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
- 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 pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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 child protection and safeguarding policy.

18. Monitoring arrangements

Behaviour and safeguarding issues related to online safety are logged in MyConcern / CPOMS, including automated alerts from Smoothwall.

This policy will be reviewed annually by the CEO. At every review, the policy will be shared with the Trust Board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

19. Links with other policies

This online safety policy does not operate in isolation and is supported by the following Trust-wide and academy-level policies:

- **Safeguarding and Student Welfare**
  - Safeguarding and Child Protection Policy
  - Anti Bullying Policy & Procedures
  - Behaviour Policy (Pupils)
  - Suspension and Permanent Exclusion Policy
  - Relationships & Sex Education (RSE)
  - Special Educational Needs
- **Technical, Systems and Data Security**
  - Acceptable Use Policies (Pupils, Staff, Parents/Carers)
  - A.I. Policy
  - Cybersecurity Policy
  - Data Protection
  - Data Retention Policy
- **Staff Conduct, Community and Operations**
  - Staff Safeguarding Code of Conduct
  - Staff Discipline Policy
  - Social Media Guidelines for Staff
  - Complaints Policy and Procedure (Trust and Academies)
  - Parent Code of Conduct
  - Educational Visits
  - Whistleblowing/Managing Allegations
  - Child protection and safeguarding policy
  - Behaviour policy
  - Staff disciplinary procedures
  - Data protection policy and privacy notices
  - Complaints procedure
  - ICT and internet acceptable use policy

Appendices

Appendix 1: Key online-safety staff

The nominated ELAT Safeguarding Trustee is Mr R Poddington

Bower Park Academy

- **Principal:** Mr Eddie Aylett
- **Designated Safeguarding Lead / Online-Safety Lead:** Mr Stuart Gander
- **LGC Safeguarding Governor:** Rebecca Templeman
- **Computing Curriculum Lead:** Mr Robert Graham
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Hall Mead School

- **Headteacher**: Miss Maria Ducker
- **Designated Safeguarding Lead / Online-Safety Lead:** Mrs Nicola Afteni
- **LGC Safeguarding Governor:** Claire Nissen
- **Computing Curriculum Lead:** Mr Kevin Lucas
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

The Brittons Academy

- **Principal:** Mrs Claire Whiley
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Laurie Cossey-Atkins
- **LGC Safeguarding Governor:** Elizabeth Dixon
- **Computing Curriculum Lead:** Ms Iyabo Aneke
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Hacton Primary School

- **Headteacher:** Mrs Emily Leslie
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Mrs Emily Leslie
- **LGC Safeguarding Governor:** Janet Daudu

- **Computing Curriculum Leads:** Rebecca Neville & Jannine Walby
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Ardleigh Green Infant School

- **Headteacher:** Mrs Verity Hoffman
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Mrs Verity Hoffman / Miss Samantha Wiley
- **LGC Safeguarding Governor:** Mrs Sandy Kirby
- **Computing Curriculum Leads:** Miss Samantha Wiley
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk

Ardleigh Green Junior School

- **Headteacher:** Mrs Janelle Johnson
- **Designated Safeguarding Lead / Online-Safety Coordinator:** Mrs Janelle Johnson / Mr Simon Harris
- **LGC Safeguarding Governor:** Mrs Sandy Kirby
- **Computing Curriculum Leads:** Mrs Charlyne Taplin
- **Network Manager / Technician:** Mr Tony Stevens / ELAT IT Helpdesk