

ACET Online Safety Policy

DATE: 28/08/26

POLICY LEAD: ACET Network Leader

APPROVED BY: Executive Team



Excellence



Equity



Empowerment

DOCUMENT CONTROL

Policy Level	Trust (Primary & Senior)	
Approved By	Executive Team	
Approval Date	2 nd September 2026	
This policy remains valid until it is reviewed and replaced; it does not expire by date alone. Policies are reviewed annually, or sooner if required by statutory or legislative changes, in line with best practice.		
Policy Lead / Author	ACET Network Leader	
Version Number	Date Issued	Updated Information
Please complete this section with a brief summary of the changes you have made or if this is a full re-write / new policy. The contents of this version control box will be shared with trustees / the LGB as part of the approval process – Thank you		
V1	28/08/26	New policy. Adopted and adapted from The Key model Online Safety Policy (September 2026) as the standalone curriculum and safeguarding online safety policy for the Trust, sitting alongside the new ICT and Internet Acceptable Use Policy and the LGfL Acceptable Use Policies (2026).

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Roles and responsibilities.....	4
3.1 The Trust Board	4
3.2 The Local Governing Board (LGB)	4
3.3 The designated safeguarding lead (DSL).....	5
3.3 The ACET Network Leader	5
3.4 The Principal.....	6
3.5 All staff and volunteers.....	6
3.6 Parents/carers	6
4. Educating pupils/students about online safety	6
4.1 Pupils/Students will be taught about online safety as part of the curriculum	6
4.2 Pupils/students will be taught practical cyber security skills.....	8
5. Educating parents/carers about online safety	9
6. Cyber-bullying.....	9
6.1 Definition	9
6.2 Preventing and addressing cyber-bullying	9
6.3 Examining electronic devices	9
6.4 Artificial intelligence	10
7. Acceptable use of the internet in the academy.....	10
8. Pupils/students using mobile devices in the academy	11
9. Staff using work devices outside the academy	11
10. How the Trust will respond to issues of misuse	11
11. Training for staff, governors and volunteers	11
12. Monitoring arrangements	12
13. Links with other policies.....	12
Appendix 1: Acceptable Use Policies.....	13

1. Aims

Our academies use a range of technology, including computers, tablets, mobile and smart devices, and internet-connected systems, as an integral part of learning, teaching and the day-to-day running of the Trust.

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils/students, staff, volunteers and governors
- Identify and support groups of pupils/students 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

This policy aims to:

- Set out expectations for staff, pupils/students, parents/carers, governors, trustees and visitors regarding safe and responsible use of technology
- Support pupils/students and staff to recognise and respond appropriately to online safety issues
- Safeguard and promote the welfare of pupils/students in accordance with Keeping Children Safe in Education 2026
- Ensure appropriate filtering and monitoring arrangements are in place, in line with DfE guidance on meeting digital and technology standards
- Set clear expectations for pupils'/students' use of mobile devices and smart technology in the academy
- Set out how the Trust will respond to online safety incidents, including cyberbullying

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

This policy should be read alongside the Trust's Child Protection and Safeguarding Policy, ICT and Internet Acceptable Use Policy, Cyber Security, Disaster Recovery & IT Incident Management Policy, Social Media Policy, AI Policy, Protection of Biometric Data Policy, and Behaviour Policy (see section 13).

2. Legislation and guidance

This policy is based on the Department for Education's statutory guidance Keeping Children Safe in Education 2026 and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying, which includes cyberbullying
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Generative AI in education
- Relationships and sex education (RSE) and health education

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It also reflects requirements in the UK GDPR and Data Protection Act 2018, the Data (Use and Access) Act 2025, the Education Act 1996 & 2011, the Equality Act 2010, the Education and Inspections Act 2006, and the Protection of Freedoms Act 2012 (in relation to biometric data).

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'/students' 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 Trust's 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 CEO and ACET Network Leader to account for its implementation.

The Trust Board will co-ordinate with the ACET Network Leader to ensure:

- The Trust meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are trained to understand their role and responsibilities around filtering and monitoring

3.2 The Local Governing Board (LGB)

The governing board has responsibility for and holding the Principal to account for its implementation at academy level.

The governing board will be assured 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 governing board will also be assured that 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 Safeguarding Governor will attend termly 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 governing board will be assured that the academy teaches pupils/students how to keep themselves and others safe, including online.

The governing board will be assured that the academy has appropriate filtering and monitoring systems in place on academy devices and academy 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 academy 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 academy's safeguarding needs

All governors will:

Make sure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school 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/students 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

3.3 The designated safeguarding lead (DSL)

Details of the DSL and deputies are set out in the Child Protection and Safeguarding Policy. The DSL takes lead responsibility for online safety, in particular:

- Supporting the ACET Network Leader with technical online safety issues
- Working with the ACET Network Leader to understand and manage filtering and monitoring systems and processes
- Providing advice and support to staff on online safety issues and taking part in interagency working where appropriate
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Managing all online safety issues and incidents in line with the academy's child protection & safeguarding policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Being aware of the potential for serious child protection/safeguarding risks arising online, including cyberbullying, radicalisation, sexual predation, and online abuse involving nudes and semi-nudes
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- 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.

3.3 The ACET Network Leader

The ACET Network Leader is responsible for the technical aspects of online safety, including:

- The academy's ICT and internet infrastructure being secure and not open to misuse or malicious attack, in line with the Cyber Security, Disaster Recovery & IT Incident Management Policy

- The Trust having appropriate filtering and monitoring systems in place, and reviewing their effectiveness
- Providing training on cyber security and online safety to staff and governors, including at induction
- Ensuring that any online safety incident with a technical cause is logged and escalated in line with the Cyber Security, Disaster Recovery & IT Incident Management Policy

Full technical detail on filtering, monitoring, password, data security and remote access arrangements is set out in the Trust's ICT and Internet Acceptable Use Policy and Cyber Security, Disaster Recovery & IT Incident Management Policy, to avoid duplication in this policy.

3.4 The Principal

The Principal is responsible for the day-to-day implementation of this policy in their academy, including ensuring staff receive appropriate training and that online safety is embedded in the curriculum.

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the Staff, Governors and Volunteers Acceptable Use Policy (LGfL, 2026)
- Working with the DSL to ensure pupils/students understand and follow this policy
- Reporting any concerns about a pupil's/student's online activity, or a colleague's conduct, to the DSL
- Modelling good practice when using technology
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the academy 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'

3.6 Parents/carers

Parents/carers are expected to notify a member of staff or the Principal of any concerns or issues regarding online safety, and to support the Trust's approach by discussing online safety with their child and reinforcing appropriate use of academy ICT systems and devices out of the academy.

4. Educating pupils/students about online safety

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

Our Academies follow the [National Curriculum computing programmes of study](#) and the government's [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for introduction 1 September 2026\)](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In relation to our Primary academies:

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 relation to our secondary academies:

In KS3, students 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

Students 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**, students 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. Students 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/students 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/students 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/students 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/students 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/students 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/students should be taught where to go for advice and support about something they have seen online. Pupils/students 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/students 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/students with SEND.

4.2 Pupils/students will be taught practical cyber security skills

All pupils/students 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/students 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 online safety issues through communications home, information evenings, and by sharing the relevant LGfL Acceptable Use Policy for their child's key stage.

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

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 academy behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils/students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils/students know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. A member of staff will discuss cyber-bullying with their classes/tutor groups.

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 academy also sends information/leaflets 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 academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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.

6.3 Examining electronic devices

The principal, and any member of staff authorised to do so by the principal, 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/students and staff. If the search is not urgent, they will seek advice from the principal/DSL.
- Explain to the pupil/student 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, the Behaviour & Rewards Policy will be followed. 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/student and/or the parent/carers 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/students 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 / searches, confiscation and use of reasonable force policy

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

6.4 Artificial intelligence

Pupils, staff and parents/carers should be aware that AI can be used to create 'deepfakes' — images, audio or video hoaxes that look real, including deepfake pornography. Any use of AI to bully, harass or create such material about another person will be treated in line with the Behaviour Policy and, where relevant, referred to the police, in accordance with the Trust's AI Policy.

7. Acceptable use of the internet in the academy

All pupils, staff, volunteers and governors are expected to sign the relevant Acceptable Use Policy before being given access to Trust ICT systems and the internet:

- LGfL Acceptable Use Policy for KS1 Pupils/students (2026)
- LGfL Acceptable Use Policy for KS2 Pupils/students (2026)
- LGfL Acceptable Use Policy for KS3 & KS4 Students (2026)
- LGfL Acceptable Use Policy for Staff, Governors and Volunteers (2026)

These are the Trust's sole acceptable use agreements and are controlled documents in their own right, appended to this policy at appendix 1. They are not duplicated elsewhere. Detailed technical acceptable use requirements for staff (password management, data security, remote access, and monitoring/filtering arrangements) are set out in the ICT and Internet Acceptable Use Policy.

Use of the Trust's internet must be for educational purposes, or for fulfilling the duties of an individual's role. The Trust monitors internet use and restricts access through filtering systems in line with the ICT and Internet Acceptable Use Policy.

8. Pupils/students using mobile devices in the academy

Arrangements for pupils'/students' use of mobile phones and smart technology (including smart watches and other wearable recording devices) are set out in the Mobile Phone Policy.

Any breach of the mobile phone/smart technology provisions may trigger disciplinary action under the Behaviour Policy, including confiscation of the device.

9. Staff using work devices outside the academy

Requirements for staff using work devices outside the academy — including device security, encryption, password requirements and reporting a lost, stolen or compromised device — are set out in full in the ICT and Internet Acceptable Use Policy, section 5, to avoid duplicating technical detail across policies.

Requirements specific to ACET-issued mobile phones, including personal use limits and data storage rules, are set out in the Work Mobile Phone Policy.

Staff members must not use a work device in any way that would breach the terms of the Staff, Governors and Volunteers Acceptable Use Policy.

10. How the Trust will respond to issues of misuse

Where a pupil/student misuses the Trust's ICT systems or internet, this will be dealt with through the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the incident, and will be proportionate.

Where a staff member misuses the Trust's ICT systems or the internet or misuses a personal device in a way that constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and staff disciplinary procedures.

The Trust will consider whether an incident involving illegal activity or content, or otherwise serious incidents, should be reported to the police, in line with the Cyber Security, Disaster Recovery & IT Incident Management Policy incident workflow.

11. Training for staff, governors and volunteers

All new staff receive training on safe internet use and online safeguarding, including cyber-bullying and radicalisation risks, as part of induction. All staff receive refresher training at least annually as part of safeguarding training, supplemented by updates through briefings, e-bulletins and staff meetings.

The DSL and deputies 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.

12. Monitoring arrangements

The Trust DSL and ACET Network Leader monitor online safety incidents and these are reported termly to the Trust Board through the safeguarding report.

The effectiveness of filtering and monitoring systems is reviewed in line with the ICT and Internet Acceptable Use Policy and Cyber Security, Disaster Recovery & IT Incident Management Policy.

This policy will be reviewed annually by the ACET Network Leader and DSL, or sooner if required by statutory or legislative changes. It is approved by the Trust Board.

13. Links with other policies

This policy is linked to the Trust's:

- Child Protection and Safeguarding Policy
- ICT and Internet Acceptable Use Policy
- Cyber Security, Disaster Recovery & IT Incident Management Policy
- LGfL Acceptable Use Policies (KS1, KS2, KS3/4, Staff/Governors/Volunteers)
- Behaviour Policy
- Staff Code of Conduct
- Social Media Policy
- AI Policy
- Protection of Biometric Data Policy
- Data Protection Policy and related privacy notices
- Mobile Phone Policy (pupils/students)
- Work Mobile Phone Policy

Appendix 1: Acceptable Use Policies

The Trust's acceptable use agreements are the LGfL Acceptable Use Policies (2026), controlled as separate documents and completed with each academy's name, logo and any local additions before issue:

- LGfL Acceptable Use Policy for KS1 Pupils
- LGfL Acceptable Use Policy for KS2 Pupils
- LGfL Acceptable Use Policy for KS3 & KS4 Students
- LGfL Acceptable Use Policy for Staff, Governors and Volunteers

These are signed at induction (staff, governors, volunteers) or at the start of each academic year (pupils), and re-acknowledged annually, in line with the implementation checklist agreed for this policy suite.