LONGTHORPE
PRIMARY ACADEMY

United in Diversity, Inspired for Life

E-Safety Policy

Keeping Pupils Safe Online

Date of Completion: November 2025
Date of Next Review: November 2026

Version 1.0

KEYS
ACADEMIES
TRUST

Contents

1. Aims

Our academy 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 academy 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 academys on:

- Teaching online safety in academyshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and academy staff
    - 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.

3. Roles and responsibilities

3.1 The Academy Committee

The Academy Committee 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 governor who oversees online safety is Dr Amaia Robles-Fernandez.

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's IT systems and the internet
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-academy 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, vITims 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 read and adhere to this policy, and that it is being implemented consistently throughout the academy.

The headteacher will make sure that the academy teaches pupils how to keep themselves and others safe, including online.

3.3 The Designated Safeguarding Lead (DSL)

Details of the academy's designated safeguarding lead (DSL) 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 academy, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher and Computing Lead 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 academy devices and academy networks
    - Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the IT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT 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 academy's child protection policy
    - Responding to safeguarding concerns identified by filtering and monitoring
    - Making sure that any online safety incidents are logged 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 academy behaviour policy
    - Updating and delivering staff training on online safety
    - Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in academy to the headteacher and/or Academy Committee
    - 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 Keys Academies Trust

Keys Academies Trust will make sure that the academy has appropriate filtering and monitoring systems in place on academy devices and academy networks, and will regularly review their effectiveness. The Trust 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

Keys Academies Trust IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on academy devices and academy 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 academy, including terrorist and extremist material
- Making sure that the academy's IT 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 academy's IT systems on a regular, ongoing 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 and dealt with appropriately in line with this 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

- Adhering to the acceptable use principles and rules, and making sure that pupils follow the academy's online safety rules
- Knowing that the Trust is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents
- Following the correct procedures by contacting the Trust IT Service if they need to bypass the filtering and monitoring systems for educational purposes (Staff only)
- Making sure that any online safety incidents are logged 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 Trust Behaviour policy and Local Academy Behaviour Protocol.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could (and does) 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
- Support the academy's online safety policy and procedures, reinforcing the expectations with their child/ren
- 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 academy's guest Wi-fi will have shared with them the Guest Wi-fi acceptable use guide. Volunteers or students that use school devices will be given a copy of the academy's acceptable use policy.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. E-safety is a curriculum area studied regularly from EYFS through to Year 6. This is achieved using the Keeping Safe Curriculum which is taught each week.

All academys have to teach:

- Relationships education and health education in primary academys
- Relationships and sex education and health education in secondary academys

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 academy**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, including when we 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing

› Why social media, computer games and online gaming have age restrITions and how to manage common difficulties encountered online

- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

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, vITims of abuse and some pupils with SEND.

5. Educating Parents/Carers About Online Safety

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

Online safety information will be promoted to parents during parents' evenings.

Upon request, the academy will let parents/carers 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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher who may then escalate to headteacher/DSL if required.

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 Trust behaviour policy and Local Academy Behaviour Protocol.)

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 vITim.

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. Class teachers will discuss cyber-bullying with their classes.

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 Trust Behaviour Policy and Local Academy Behaviour Protocol. 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 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 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 headteacher/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 academy 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.

Longthorpe Primary Academy 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.

Longthorpe Primary Academy will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using freely available AI tools while they are still being developed. Any information that could pose a data protection risk, must not be entered into such AI systems.

AI tools that are commissioned by the school for use or as part of an existing subscription package, may be used in line with the academy's policies and procedures.

Any use of artificial intelligence should be carried out in accordance with guidance from the Academies Trust.

7. Acceptable use of the internet in academy

All pupils, parents/carers, staff, volunteers and governors are expected to adhere to the acceptable use policy.

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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict IT access through filtering systems where appropriate.

More information is set out in the Acceptable Use policy.

Year 6 parents/carers are required to sign an iPad agreement which outlines the usage of the provided academy devices which outlines the use and care of these devices.

8. Pupils using home devices in academy

Pupils may bring mobile devices into academy, but are not permitted to use them during:

- Lessons

- Clubs before or after academy, or any other activities organised by the academy
- Parents are informed that devices with the ability to take photographs or make phone calls e.g smart watches, are not permitted in academy

Pupils who wish to bring a mobile device into academy will hand these to the class teacher to be securely stored away until the end of the day.

Any unacceptable use of IT by a pupil may trigger disciplinary action in line with the Trust Behaviour Policy and Local Academy Behaviour Protocol, which may result in the confiscation of their device.

Longthorpe Primary Academy will not be held liable for any damage or misuse of personal devices brought into the academy.

9. Staff using work devices outside academy

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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 promptly installing the latest updates

Staff members must not use the device in any way that would violate the academy's terms of acceptable use policy or Code of Conduct.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT manager through the employee portal.

10. How the academy will respond to issues of misuse

Where a pupil misuses the academy's IT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's IT 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 Code of Conduct and the Trust Disciplinary Rules and Procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will determine, on a case-by-case basis, whether any incident involving illegal activity, illegal content, or other serious misconduct must be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff, governors and volunteers will receive this policy and are required to evidence that they have read and understood it as part of their induction.

All staff members will receive relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL, DDSLs 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.

11.2 Pupils

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 training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety through the platform MyConcern.

This policy will be reviewed every year by the Safeguarding team and the Computing Lead. At every review, the policy will be shared with the academy committee.

13. Links With Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy