



Online Safety Policy

2026-27



Contents

Contents	2
Aims	3
Waterton Academy Trust Aims to:.....	3
The 4 Key Categories of Risk	3
Legislation and Guidance	3
Roles and Responsibilities	4
Trustees and the Academy Standards Committee	4
The Headteacher	5
The Designated Safeguarding Lead	5
IT Services Manager	6
All Staff and Volunteers	7
Parents/Carers.....	7
Visitors and Members of the Community.....	8
Educating Pupils About Online Safety.....	8
Educating Parents/Carers About Online Safety.....	9
Cyber-Bullying	9
Definition.....	9
Preventing and Addressing Cyber-Bullying.....	10
Examining Electronic Devices.....	10
Artificial Intelligence.....	11
Acceptable Use of the Internet	12
Remote Education and Live Streaming.....	13
Pupils Using Mobile Devices.....	13
How the Academy Will Respond to Issues of Misuse	13
Training.....	13
Monitoring Arrangements	14
Links With Other Policies	15
Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)	16
Acceptable Use of the Academy's ICT Systems and Internet: Agreement for Pupils and Parents/Carers.....	16
Appendix 2: KS2 Acceptable Use Agreement (Pupils and Parents/Carers).....	17
Acceptable Use of the Academy's ICT Systems and Internet: Agreement for Pupils and Parents/Carers.....	17
Appendix 3: Online Safety Training Needs – Self-Audit for Staff	18
Online Safety Training Needs Audit.....	18
Document Detail.....	19
Version Control.....	19

Aims

Waterton Academy Trust 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 trust community in its use of technology, including mobile phones, smart watches, camera-enabled wearable devices (such as smart glasses), and other connected technologies.
- Establish clear mechanisms to identify, intervene and escalate any incidents using all available external agencies to maximise outcomes, where appropriate.
- Bring awareness to pupils and adults as to the current online risks to their safety and emotional wellbeing and foster a culture of self-resilience, awareness and responsible use of digital technologies.

The 4 Key Categories of Risk

Our trust-wide approach to online safety is based on addressing the following categories of risk outlined in Keeping Children Safe in Education (KCSIE 2026):

- Content – Being exposed to illegal, inappropriate or harmful online content, including pornography, fake news, misinformation, disinformation, conspiracy theories, racism, misogyny, misandry, self-harm, suicide, antisemitism, radicalisation, extremism, and extreme sexual or physical violence.
- Contact – Being subjected to harmful online interaction with other users or generative AI applications that simulate this interaction, including peer pressure, commercial advertising, online scams, and adults posing as children or young adults with the intention to groom, exploit or radicalise children for sexual, criminal, financial or other purposes.
- Conduct – Online behaviour that increases the likelihood of, or causes, harm, including bullying, abusive or harassing behaviour, sexual harassment, sharing explicit or abusive content, consensual and non-consensual sharing of self-generated intimate images and/or videos including those generated using AI (e.g. deepfakes), online misogyny, image-based abuse, upskirting, initiation/hazing behaviours and harmful sexual behaviour.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The Trust recognises that online harm often intersects with risks within the local community, peer groups and wider social environments. Online activity will therefore be considered alongside offline experiences when assessing safeguarding risk.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance and advice, including:

- *Keeping Children Safe in Education* (DfE, September 2026)

- *Behaviour in Schools: Advice for Headteachers and School Staff* (DfE, February 2024)
- *Filtering and Monitoring Standards* (DfE, March 2023)
- *Mobile Phones in Schools: Guidance for Headteachers* (DfE, February 2024)
- *Teaching Online Safety in Schools* (DfE, June 2019)
- *Preventing and Tackling Bullying: Advice for Headteachers, Staff and Governing Bodies* (DfE, July 2017)
- *Searching, Screening and Confiscation* (DfE, 2023)
- *Working Together to Safeguard Children* (DfE, July 2026)
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE, 2019, updated 2021)

This policy also reflects relevant legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, and the Education Act 2011.

It also takes into account:

- The National Curriculum computing programmes of study
- Guidance from the National Crime Agency's CEOP Education programme (<https://www.thinkuknow.co.uk>)

This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

Trustees and the Academy Standards Committee

Members of each Academy Standards Committee (ASC) have devolved responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The ASC 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.
- 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.
- will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trustees will:

- ensure that each academy has appropriate filtering and monitoring systems in place on academy devices and networks and will regularly review reports of their effectiveness.

The Executive Leadership Team (ELT) will:

- review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support each academy in meeting those 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 their safeguarding needs.

All governors and trustees will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (See Acceptable Use Policy)
- Ensure that online safety is fully considered while devising and implementing any whole school or whole trust approach to safeguarding alongside any related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and 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.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is implemented consistently throughout the academy.

The Designated Safeguarding Lead

Details of the academy's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as within relevant job descriptions. The DSL will work with safeguarding partners, police and children's social care where online safeguarding concerns indicate significant harm, exploitation, radicalisation or criminal activity, ensuring that referrals are made in accordance with local safeguarding partner arrangements.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on academy devices and academy networks.
- Review filtering and monitoring reports and ensure escalation routes are in place when harmful patterns are detected, including to the Headteacher, Trust safeguarding team, and external agencies where necessary.
- Working with the IT Services manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, IT Services 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 safeguarding and child protection policy.

- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy and the safeguarding and child protection policy.
- Ensuring 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the headteacher and/or ASC.
- Undertaking annual risk assessments that consider and reflect the risks children 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.

IT Services Manager

The IT Services manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on academy devices and networks, which are reviewed and updated at least annually to assess effectiveness, and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the trust / academy 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 trust / academy ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- When required, reviewing any online safety incidents or cyber-bullying incidents logged on CPOMS.

This list is not intended to be exhaustive.

Filtering and monitoring systems will be reviewed at least annually and following any significant safeguarding incident or technological change.

Reviews will:

- assess effectiveness across all internet-connected devices and locations
- consider the age range and vulnerability of pupils
- evaluate emerging online risks
- include checks that filtering systems are functioning correctly
- ensure escalation routes are understood by relevant staff
- be recorded and retained as part of safeguarding governance evidence

Filtering and Monitoring Governance

The Trust Board retains strategic responsibility for ensuring appropriate filtering and monitoring arrangements are in place across all academies and that these are reviewed regularly as part of safeguarding governance.

The Headteacher is responsible for ensuring the effective implementation of filtering and monitoring arrangements within the academy and for ensuring that safeguarding concerns arising from these systems are responded to appropriately.

The Designated Safeguarding Lead (DSL) has operational safeguarding oversight of filtering and monitoring systems, including reviewing monitoring reports, identifying safeguarding risks, ensuring appropriate action is taken, and escalating concerns where necessary in line with the Child Protection and Safeguarding Policy.

The IT Services Manager is responsible for the technical operation, maintenance, testing and ongoing effectiveness of filtering and monitoring systems, working in partnership with academy leaders and the DSL to ensure systems remain appropriate, proportionate and effective.

Trustees, the Executive Leadership Team and Academy Standards Committees will receive regular assurance regarding the effectiveness of filtering and monitoring arrangements, including safeguarding incidents, testing outcomes, identified risks and actions taken to address any weaknesses.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (See Acceptable Use Policy) and ensuring that pupils follow the academy'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 informing the DSL.
- Following the correct procedures by contacting the DSL and the trust IT Services Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy 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'.
- Staff are expected to model safe, respectful and responsible online behaviour at all times, in line with the DfE Behaviour in Schools (2024) guidance and the Trust's Employee Code of Conduct.

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy'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](#)
- Hot topics - [Childnet International](#)
- Parent resource sheet - [Childnet International](#)

Visitors and Members of the Community

Visitors and members of the community who use the trust / academy ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (See Acceptable Use Policy).

Visitors, contractors, parents/carers and other members of the community must not use camera-enabled wearable devices, including smart glasses, to capture images, video or audio whilst on Trust premises without the explicit permission of the Headteacher. Where there are safeguarding, privacy or data protection concerns, visitors may be asked to remove or disable such devices before entering the school.

Educating Pupils About Online Safety

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

All academies have to teach:

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

In Key Stage 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 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.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when 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 is shared and used online

- How to identify misinformation, disinformation, manipulated content, synthetic media and conspiracy theories online
- How algorithms, influencers, advertising and AI-generated content may influence beliefs, behaviours and decision-making
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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

Online safety teaching will be adapted for pupils with SEND, those with communication difficulties, and those identified as particularly vulnerable, ensuring accessibility and equity of provision. In addition, where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children or victims of abuse.

Pupils affected by harmful online experiences will be offered access to pastoral and mental health support, in line with DfE guidance on Mental Health and Behaviour in Schools (2021).

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.

Online safety will also be covered during parents' evenings.

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 headteacher and/or the DSL.

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

Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy behaviour policy and anti-bullying policy.)

The Trust recognises that harmful online behaviour may exist on a continuum from inappropriate comments and misogynistic language through to sexual harassment, coercion, image-based abuse and sexual violence.

Such behaviour will never be dismissed as “banter”, “part of growing up” or “just having a laugh”. All concerns will be treated seriously and responded to as safeguarding matters where appropriate.

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 are encouraged 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. Teachers will discuss cyber-bullying with their class.

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.

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 headteacher.
- Explain to the pupil why they are being searched, 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 and headteacher 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 if 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/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 self-generated intimate images and/or videos including those generated using AI e.g. deepfakes) 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](#)

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

Racist or discriminatory online incidents will be reported to the Local Authority as required. Serious criminal matters will be referred to the police, and safeguarding concerns to children's social care, in line with KCSIE 2026.

Artificial Intelligence

The Trust recognises that generative artificial intelligence (AI) tools are increasingly used by both adults and children. AI may support learning, creativity and accessibility, but also presents safeguarding, ethical, data protection and online safety risks.

Risks associated with AI may include:

- exposure to harmful, biased, extremist or inappropriate content
- inaccurate or misleading information
- misinformation and disinformation
- impersonation or manipulation of others
- AI-generated sexualised or abusive imagery, including deepfakes
- online sexual harassment and image-based abuse
- plagiarism or academic misconduct
- unsafe sharing of personal data or confidential information
- exploitation through AI-enabled scams or grooming

The Trust will:

- educate pupils about the safe and responsible use of AI tools
- ensure staff understand safeguarding risks linked to AI
- assess AI tools before educational use where appropriate
- ensure appropriate human oversight remains in place where AI is used to support learning, assessment or administration.
- ensure filtering and monitoring systems appropriately address AI-related risks
- respond to AI-related safeguarding concerns in line with the Child Protection and Safeguarding Policy
- ensure AI use complies with data protection, safeguarding and staff conduct expectations

Staff and pupils must not use AI tools to create, access, share or manipulate harmful, abusive, discriminatory, explicit or illegal content.

Use of AI by Pupils

- Pupils are not permitted to use Artificial Intelligence (AI) tools in school.
- We recommend that parents and carers do not allow children to use AI tools at home without adult supervision. AI systems can produce harmful, misleading or inappropriate content that children may not recognise.
- AI must never be used by pupils to create or share harmful, bullying or inappropriate content. Such incidents will be dealt with under the Behaviour and Anti-Bullying Policies.

Employee Use of AI

The use of Artificial Intelligence (AI) by staff is governed by the Waterton Academy Trust AI Policy. This sets out expectations for safe, ethical and appropriate use of AI in supporting staff with administration tasks. Staff must follow the AI Policy at all times and seek advice from their line manager or the Trust's safeguarding/IT leads if unsure.

Acceptable Use of the Internet

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1 to 2 and the Acceptable Use Policy). Visitors will be

expected to read and agree to the academy's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1 to 2 and the Acceptable Use Policy

Remote Education and Live Streaming

Where remote education, online meetings or live-streamed learning are used, the academy will ensure appropriate safeguarding arrangements are in place, including:

- use of approved platforms
- appropriate staff supervision
- professional conduct expectations
- safeguarding reporting arrangements
- appropriate filtering and monitoring controls where possible

Pupils Using Mobile Devices

Pupils should not bring mobile phones, smart watches, camera-enabled wearable devices (including smart glasses), or other internet-connected personal devices into school except with prior agreement of the Headteacher. Phones/smart watches will be kept in the school office during the school day. The Trust expects all academies to operate as mobile phone-free environments by default throughout the school day.

How the Academy Will Respond to Issues of Misuse

Where a pupil misuses the academy's ICT 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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. This is available through Flick Learning which all staff have access to.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Staff training will include awareness of emerging technologies, including AI-enabled devices and camera-enabled wearable technology, so staff understand the safeguarding, privacy and data protection implications and know how to respond appropriately.

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.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed every year by the trust. At every review, the policy will be shared with Trustees and with the Academy Standards Committee.

We work with a range of external agencies to provide support for pupils with SEND. These services include, but are not limited to:

- Speech and language therapists
- Specialist teachers or support services
- Educational psychologists
- Occupational therapists, speech and language therapists or physiotherapists

- General practitioners or paediatricians
- School nurses
- Child and adolescent mental health services (CAMHS)
- Education welfare officers
- Social services

Online safety incidents and concerns, including breaches of filtering/monitoring, will be recorded on CPOMS. Data will be analysed at Trust level to identify patterns (e.g., repeat victims, persistent perpetrators, or incidents linked to protected characteristics) and reported to trustees.

Links With Other Policies

This Online Safety Policy is linked to the following Trust policies:

- **Child Protection and Safeguarding Policy**
- **Behaviour Policy**
- **Anti-Bullying Policy**
- **Acceptable Use Policy and**
- **Staff Code of Conduct**
- **Code of Conduct for Parents, Carers and Visitors**
- **Abusive or Threatening Behaviour Policy**
- **Data Protection**
- **Complaints Policy**

Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

Acceptable Use of the Academy's ICT Systems and Internet: Agreement for Pupils and Parents/Carers	
Name of Pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carers • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (Pupil)	Date:
Parent/Carer Agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (Parent/Carer)	Date:

Appendix 2: KS2 Acceptable Use Agreement (Pupils and Parents/Carers)

Acceptable Use of the Academy's ICT Systems and Internet: Agreement for Pupils and Parents/Carers	
Name of Pupil:	
I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it I will not: • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (Pupil)	Date:
Parent/Carer Agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (Parent/Carer)	Date:

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

Online Safety Training Needs Audit	
Name of Staff Member/Volunteer:	Date:
Question	Yes/No
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Do you understand the risks of pupils using Artificial Intelligence (AI) tools (e.g. deepfakes, harmful content, academic misuse)? Are you confident about how to respond if a pupil misuses AI in or out of school?	
Do you know what the DfE Filtering and Monitoring Standards (2023) require of schools? Do you know how to escalate concerns if filtering/monitoring systems are not working effectively?	
Are you confident in recognising online sexual harassment, image-based abuse, upskirting, hazing, or initiation behaviours as safeguarding issues?	
Are you aware of the Trust's rules for mobile phones, smart watches, and personal devices in school? Do you know how to respond if these devices are misused?	
Are there any areas of online safety in which you would like training/further training?	

Document Detail			
Document Name:		Online Safety Policy	
Version:		4	
Chief Officer Signature:		D Dickinson, CEO	
Effective From:		September 2026	
Approved by:		Executive Leadership Team	
Next Review Date:		Sept 2027	
Version Control			
Version	Date	Author	Change/Reference
1	July 2023	M Bretherton / D Dickinson	New Policy
2	Sept 2024	M Bretherton	No Changes
3	Sept 2025	M Bretherton	Statutory references updated; risks, monitoring, staff culture, pupil support, parental conduct and reporting strengthened. New section on AI added.
4	July 2026	M Bretherton	Updated in line with KCSIE 2026 draft proposals, including: - strengthened safeguarding language relating to harmful sexual behaviour, misogyny and online sexual harassment - updated terminology relating to self-generated intimate images, AI-generated content and deepfakes - expanded Artificial Intelligence (AI) section to address safeguarding, misinformation, impersonation, data protection and ethical risks - strengthened filtering and monitoring governance, review and escalation expectations - added clearer expectations regarding mobile phone-free environments - expanded online risk categories to include misinformation, disinformation,

			conspiracy theories and AI-enabled harms - strengthened curriculum expectations around digital literacy and identifying manipulated content - added remote education and live-streaming safeguarding expectations - updated references and terminology to align with KCSIE 2026 consultation draft and related DfE guidance. - Additions in relation to smart glasses.
--	--	--	---