'They will soar on wings like eagles …'
Isaiah 40:31

collaborate | enrich | trust | innovate | aspire | nurture

AQUILA Diocese of Canterbury Academies Trust

Multi Academy Trust Policy

Common Trust Policy, Use as Published

Online Safety Policy

Date adopted by Trust Board: 07/2023

Date of Review: 10/2024

Date of next Review: 10/2025

Version	Date	Author	Change Description

Contents

1. Aims

Information and Communication Technology (ICT) is integral to the way our Trust works and is a critical resource for pupils, staff, trustees, governors, volunteers, and visitors. It supports teaching and learning, pastoral and administrative functions of the schools.

However, the ICT resources and facilities our schools use also pose risks to data protection, online safety, and safeguarding.

Through this policy, the Trust aims to ensure that each school:

- Has robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors at school level.
- Delivers 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').
- Establishes 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – Being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct** – Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images, and online bullying.
- **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 (2024)** and its advice for schools on:

- Teaching Online Safety in Schools
- Preventing and Tackling Bullying and Cyber-Bullying: Advice for Headteachers and School Staff
- Relationships and Sex Education
- Searching, Screening, and Confiscation at School

It also refers to the DfE's guidance on **Protecting Children from Radicalisation** and reflects the provisions of the **Online Safety Act 2024**.

It reflects existing legislation, including but not limited to:

- Education Act 1996
- Education and Inspections Act 2006
- Equality Act 2010
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018

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 Trust Board and Local Governing Bodies

The Trust Board has overall responsibility for all pupils within the Trust. ICT and online safety are delegated to the Local Governing Bodies (LGB) of each school. As such, the Trust Board will monitor this policy and its impact across the Trust. LGBs have responsibility for holding their Headteachers to account for its implementation.

Trustees will:

- Review the policy to ensure compliance and effectiveness within the Trust context.
- Take an overview of online safety throughout the Trust and consider the effectiveness of online safety provisions.
- Monitor emerging online risks, such as AI-driven online abuse, deepfake technology, and algorithmic manipulation, as outlined by the Online Safety Act 2024.
- Ensure annual digital safeguarding audits are conducted to assess each school's readiness to handle new types of digital threats.

This list is not intended to be exhaustive.

Governors will:

- Ensure that 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.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and procedures.
- Ensure that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse, and pupils with special educational needs and/or disabilities (SEND).
- Monitor the implementation of updated roles and responsibilities concerning online safety.

This list is not intended to be exhaustive.

3.2 Senior Leaders (CEO, Headteacher, Head of School)

The Trust CEO will:

- Take an overview of online safety practices and promote opportunities to share resources and improve practice in line with this policy.
- Ensure all schools within the Trust have access to relevant cyber protection tools and filtering systems that now cover real-time risk assessment of new digital trends (e.g., apps, platforms).

This list is not intended to be exhaustive.

The Headteacher is responsible for:

- Ensuring that staff understand this policy and implement it consistently throughout the school.
- Working with the Designated Safeguarding Lead (DSL) to address any online safety issues or incidents.
- Ensuring that the school's response to online safety is dynamic and reacts to new threats in the digital ecosystem.

This list is not intended to be exhaustive.

3.3 Designated Safeguarding Lead (DSL)

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, ICT Support Provider, and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Trusts child protection & safeguarding policy.
- Ensuring that any online safety incidents are logged (see Appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying or AI-related incidents are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety, including emerging risks like AI-generated content and advanced cyber-scams (see Appendix 1 for a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.

This list is not intended to be exhaustive.

3.4 ICT Support Provider

The ICT Support Provider will:

- Put in place an appropriate level of security protection procedures.
- Update all content-filtering and monitoring systems to account for emerging online threats.
- Conduct risk reviews, ensuring the school's digital infrastructure can handle threats effectively.
- Ensure that the school's ICT systems are secure and protected against viruses, malware, and emerging threats and are updated regularly.
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.
- Ensure that any online safety incidents are logged (see Appendix 2) and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying or advanced cyber-scams are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors, 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 school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying or exposure to new online risks are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment both online and offline, maintaining an attitude of 'it could happen here'.
- Participating in annual refresher training on emerging technologies, such as AI, as part of the school's safeguarding training regime.

This list is not intended to be exhaustive.

3.6 Parents and Carers

Parents and 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 school's ICT systems and internet.

- Support the school in educating their children about online safety, including the risks associated with AI-generated content, advanced cyber-scams, and data privacy.
- Seek further guidance on keeping children safe online from the following organisations and websites:

    - **UK Safer Internet Centre** – What are the issues?
    - **Childnet International** – Hot topics
    - **Childnet International** – Parent resource sheet

4. Educating Pupils About Online Safety
Pupils will be taught about online safety as part of the curriculum.
All schools are required to teach, Relationships Education and Health Education in primary schools.

In Key Stage 1 and 2, 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.
- Recognise acceptable and unacceptable behaviour.
- Understand the risks posed by strangers or others online, including those who might seek to build relationships to exploit or abuse them.
- Critically evaluate the content they see online, including understanding that some content is deliberately misleading.

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.
- 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.

New Areas of Focus:

- AI Awareness: Educating pupils about AI-generated content, such as deepfakes, and how to critically assess the authenticity of online media.
- Data Privacy: Emphasising the importance of safeguarding personal data across all platforms and understanding privacy settings.
- Algorithm Literacy: Helping students understand how algorithms shape the content they see online and the potential risks involved.

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, and some pupils with SEND.

Educating Parents About Online Safety
The school will raise parents' awareness of internet safety through:

- Letters, newsletters, and other communications home.
- Information and resources on our website.

- Parent workshops and information sessions during parents' evenings.

The school will inform parents about:

- What systems the school 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 school (if anyone) their child will be interacting with online.
- The latest online risks, including AI-generated content, advanced cyber-scams, and data privacy concerns.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-Bullying

6.1 Definition

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

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, the school will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. Pupils will be encouraged to report any incidents, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take, including new forms like AI-generated harassment, and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.
Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including PSHE education and other subjects where appropriate.
All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, ways to support pupils, and emerging online risks as part of safeguarding training.
The school also provides information and resources on cyber-bullying to parents so that they are aware of the signs, how to report it, and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police and will work with external services if necessary.

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 school 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.
- 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 cooperation.

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 been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the school 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 or 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 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 immediately, who will decide what to do next, following the DfE's latest guidance on **Searching, Screening and Confiscation at School** 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 at School**.
- 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 school complaints procedure.

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. These documents can be found in our ICT Security Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

The school, with the support of its ICT Support Provider, will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

8. Pupils Using Mobile Devices in School

Pupil access to the internet will be limited to ICT-based lessons and using the equipment available in school. Students will not have the ability to access the school internet via any personal devices.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Exceptions:

The only exception will be pupils using a mobile device to manage a known medical condition where tracking requires access to a specific app. In this case, due to the potential safeguarding risks to other pupils, the school and parents must have explored and rejected all alternatives, a full risk assessment must be completed and agreed upon (see Appendix 3), and the school must be satisfied that cameras, other apps, and access to messaging are disabled.

9. Staff Using Work Devices Outside School

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. Passwords should be at least 10 characters long, contain a number and at least one capital letter, and be updated every 90 days.
- 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 required by the school.
- Keeping operating systems up to date by always installing the latest updates.
- Being vigilant against phishing attempts and other cyber-scams.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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 Headteacher, who will liaise with the school ICT Support Provider.

10. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and the ICT Security 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 school'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. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

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

11. Training

All new staff members will receive training as part of their induction on safe internet use and online safeguarding issues, including cyber-bullying, the risks of online radicalisation, and emerging threats like AI-generated content.

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.
- New online risks, such as AI-generated content (deepfakes), advanced cyber-scams, and algorithmic manipulation.

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 two 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 DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 2.

This policy will be reviewed every year by the Trust Board. At every review, the policy will be shared with the LGBs. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology and the risks and harms related to it evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Handbook
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT Security Policy

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
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 and parents?	
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?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3 – School Risk Assessment

School Risk Assessment

In this case this assessment ***MUST*** be shared with the parent	**Risk Description**	**Action Requirements**
	High Risk	Risk will be actively managed with strong control measures.
	Medium Risk	Monitor and take appropriate action to reduce risk.
	Low Risk	Risk to be monitored and assessed ongoing.

Location, activity, or issue being looked at: Medical Mobile phone access in school for medical needs

Date of activity:

REMEMBER to Risk Assess the Activity / the Setting / the Group
The WHAT The WHERE The WHO

Activity or Task Being Assessed.	Hazard/Concern (something with the potential to cause harm) **What could go wrong?**	**Who may be harmed?**	Risk Rating **RAG**	**What is being done**, that helps control/manage the risk?	Risk Rating **RAG**	What **extra controls** need to be put in place?	**By when?**	**By whom?**
Mobile phone in school for tracking known medical condition – child with access	Inappropriate apps or content being accessed or shared on the phone **The sole use of the device in school is for monitoring medical purposes**	Children Staff		Phone only has the technology needed for their health care installed – other applications on the mobile phone to be deactivated. The phone MUST stay with an adult at all times – Child can regularly check their blood sugar levels on their phone throughout the school day. This will be closely monitored by a trained adult/First Aider. Parents to provide access code to the phone: _____ Parents to provide the school with access to internal code on phone – such as screen time on an iPhone:		ALL other apps disabled each day BEFORE arriving at school. Staff to check the apps are disabled daily. Issues to be logged in contact book On arrival at school / Breakfast Club, the device is handed directly to staff, who will then give to classroom staff to make any necessary checks School to continue work educating pupils and parents about the safe use of social media. We embed online safety throughout our curriculum and assemblies.	Each day	Class adult trained adult

				By signing this document parents and child agree to school staff accessing the phone and making any necessary changes required to safeguard both pupils and staff.				
Mobile phone in school – Access to the school's Internet connection	School network is accessed and compromised	Children Staff School		The school provides a network connection, with permission, to connect their personal devices to the Internet – 'medical' Network to be set at 'pupil level' to protect the user, will be locked down as much as possible and regularly monitored The school does not permit the downloading of apps or other software whilst connected to the school network and the school is not responsible for the content of any downloads onto the user's own device whilst using the school's network.		Access to the network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately at any time. NB-The school cannot guarantee that the wireless network is secure or will be available at all times, users use it at their own risk. Parents/users need to have a contingency in the event that the school network is not available	By time phone is connected to school network	Class adults and IT technician
Mobile phone in school – Monitoring the use of mobile devices	Other apps are accessed and used within school hours	The school network and systems		The school reserves the right to use technology that detects and monitors the use of personal devices, which are connected to or logged on to our network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and school information. Keeping children safe in education 2023 (publishing.service.gov.uk)		Any inappropriate access/content received through school IT services or the school internet connection should be reported to the Headteacher / Designated Safeguarding Lead as soon as possible. **Filtering and Monitoring** As part of this process, governing bodies and proprietors should ensure their	By time phone is connected to school network	SLT and IT technician

						school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness.		

Agreed and signed by parents Signature: _____ _____ Role: _____ _____ Date:_____ _____	**Signed on behalf of school Leadership:** Signature: _____ Role: _____ Date:_____