'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 next Review: 07/2024

Contents

Contents

1. Introduction

All Souls' is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to both educate and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

2. Aims

ICT is an integral part of the way 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 school.

However, the ICT resources and facilities our school uses 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
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

In line with Keeping Children Safe in Education, we aim to address the following four areas 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, anti -Semitism, 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; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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 e-safety is delegated to the Local Governing Body (LGB) of each school. As such, the Trust board will take an oversight of monitoring this policy and its impact across the trust, LGBS have responsibility for holding their Head Teacher to account for its implementation.

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

Trustees will:

- Review the policy annually to ensure compliance and effectiveness within the trust context.
- Take an overview of e-safety throughout the trust and consider the effectiveness of e-safety provisions.
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated

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 students are taught about online safety
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

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

The Trust CEO will take an overview of e-safety practices and promote opportunities to share resources and improve practice in line with this policy.

The Head Teacher is responsible for ensuring that staff understand this policy, and ensure that it is implemented consistently throughout the school and ensuring any new members of staff learn about our approach to online safety at induction and regularly thereafter.

The Headteacher will understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns.

3.3 The designated safeguarding lead

Details of the school'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 school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Oversee the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead
- Working with the Head Teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents in line with the safeguarding policy
- Managing all online safety and cyber-bullying issues and incidents in line with the school child protection policy

- Updating and delivering staff training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary including children's social care and the police and make referrals with the support of relevant colleagues and their expertise
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received
- Providing regular reports on online safety in school to the Head Teacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Support provider will (if not appropriate delete and add bullet points to headteacher)

- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the school's ICT systems are secure and protected against viruses and malware
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers will:

- Assist with the consistent implementation of this policy by agreeing with 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.
- Read and understand this policy
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Work with the DSL to 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 are dealt with appropriately in line with the school behaviour policy
- Respond 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'
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.

This list is not intended to be exhaustive.

3.6 Parents

Parents and carers will

- Understand the importance of children being safe online

- Read, understand and comply with this policy
- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access and who from the school (if anyone) will be interacting with their child
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online

4. Educating pupils about online safety

In line with 'Teaching online safety in school,' published by the Department for Education in June 2019, we teach pupils about online safety and harms. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives, Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools

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
- 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.

We recognise that there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. Such groups may also face additional risks, for example from bullying, grooming and radicalisation.
We will ensure these pupils receive the information and support they need through additional learning or more frequent reminders.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents know:

- 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,

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL.

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

6. Filtering and monitoring

6. Filtering and Monitoring

School uses Netsweeper as a filtering and monitoring system. This filters and monitors for unsuitable websites and contents . This covers our school network and the following devices:tablets, laptops, desktops and mobile devices.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies monitor the effectiveness of this system through the reports they receive.

The school takes care to not 'over block; content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

The DfE has published filtering and monitoring standards which set out that schools should:

- **Identify and assign roles and responsibilities to manage filtering and monitoring systems**
- **Review filtering and monitoring provision at least annually**
- **Block harmful and inappropriate content without reasonable impacting teaching and learning**
- **Have effective monitoring strategies in place that meet their safeguarding needs**

We at School have done the following in relation to this: Made sure netsweeper is upto date and any standalone devices have the netsweeper certificate install on them and an IP address is reserved to help with tracking.

When the filtering and monitoring system detects concerning usage, we will record this and take appropriate action, including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact…the school office , who can put you through to the correct advice

7. Cyber-Bullying

7.1 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 school behaviour policy.)

7.2 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 are encouraged to do so, 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 and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets 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 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.

7.3 Examining electronic devices

The Head Teacher, and any member of staff authorised to do so by the Head Teacher as set out in our behaviour policy, 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, 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 / Head Teacher / other member of the senior leadership team] 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 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

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

8. 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.

9. 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 brought in devices.

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, could sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To manage this and reduce risk, we ensure all pupils hand their mobile phones to the school at the start of the school day. The phones are collected by the pupil at the end of the school day.

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.

10. 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 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

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.

11. 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, 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.

12. 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.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.
- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online, this can take the form of:
    - Online abuse, including sexual
    - Online harassment, including sexual
    - Cyberbullying
    - Misogynistic/ misandrist messages,
    - the non-consensual sharing of incident images, especially around chat groups,
    - and the sharing of abusive images and pornography to those who do not want to receive such content.

- That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

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).

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.

13. Further Information to support you.

We work with our local safeguarding partners to ensure our students are safeguarding. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For **parents** the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- Thinkuknow- how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For **students** the following websites could be of use:

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For **all staff and volunteers** it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- UK Safer Internet Safety- teacher guides and resources
- https://www.internetmatters.org/schools-esafety/
- https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy.
- Behaviour policy.
- Staff Code of Conduct inc. acceptable use of technology in the staff behaviour policy/ code of conduct.
- Anti-bullying procedures including cyberbullying
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in schools and colleges (DfE)

14. Monitoring.

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 LGB's. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online (such as the one available here). This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. 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**