St. Anthony's Girls' Catholic Academy

Online Safety Policy

Policy updated: June 2024

Policy Review: June 2025

Signed by: M. A. Galbraith

Chair of Governors

1. **Context**

Our Online Safety Policy outlines the commitment of St Anthony's Girls' Catholic Academy to safeguard members of our school community online in accordance with statutory guidance and best practice. This Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers and visitors) who have access to and are users of school ICT systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). St Anthony's Girls' Catholic Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy was developed by governors and teachers, in partnership with parents and pupils, considering our Mercy ethos and local and national policy and guidance.

2. Aims

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- 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;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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 scam

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for

and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

4. Curriculum

Pupils are taught about online safety each year as part of the ICT curriculum in **Key Stage 3**, and in the Personal Development curriculum in **Key Stages 3-5**.

Pupils are taught:

- To understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- To recognise inappropriate content, contact and conduct
- To understand the importance of limiting screen time in terms of health and wellbeing.
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- The impact of viewing harmful content.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, and how and when consent can be withdrawn (in all contexts, including online)
- How to report a range of concerns, as well as what to do and where to get support to report material or manage issues online.

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

We also use opportunities to reinforce learning and understanding through national initiatives such as 'Safer Internet Day' where appropriate.

5. Roles and Responsibilities

All governors and staff sign an 'Acceptable Use of ICT Systems Policy agreement' annually and all students and parents sign an 'Acceptable Home-Academy agreement' detailing ICT, mobile phone and Bring Your Own Device policies. Additionally, key staff have further responsibilities:

Headteacher/Designated Safeguarding Lead

- provide clear and specific directions to staff and volunteers on how to behave online
- provide support, information and encouragement for parents and carers to do what they can to keep their children safe online
- develop an online safety agreement for use with young people and their parents/carers
- provide supervision, support and training for staff and volunteers about online safety
- develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

ICT manager and support staff

- maintain and monitor a keyword-based active monitoring system to identify possible issues.
- review and update the security of our information systems regularly.
- perform regular checks of the active monitoring system logs and record any concerns.
- identify when major issues are developing and report them to the Headteacher/Designated Safeguarding Lead.
- ensure devices connected to the school network utilise a filtered connection that blocks access to inappropriate content and logs attempts to access it.
- ensure personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.

Staff

- adhere to the Acceptable Use of ICT agreement.
- ensure that usernames, logins, email accounts and passwords are used effectively.
- ensure that images of children, young people and families are used only where photo consent has been given.
- examine and risk assess any social media platforms and new technologies before they are used within the organisation.
- support and encourage young people to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- report any concerns immediately to the Designated Safeguarding Lead.

Students

- adhere to the Acceptable Use of ICT agreement.
- ensure that usernames, logins, email accounts and passwords are used effectively.
- Only use software and/or websites as directed by the member of staff
- report any concerns immediately to a member of staff.

Parents

- The academy will raise parents' awareness of internet safety in letters, newsletters or other communications home, and in information via our website and social media. This policy will also be shared with parents.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of House.

6. ICT systems and Infastructure

We have a robust system in place to ensure the online safety of pupils, staff, volunteers and governors:

1. **Senso** is our IT classroom management tool which allows for control and monitoring of every computer in the school. Staff may use this to monitor lessons, interact with student ICT devices and temper usage of ICT in real time within lessons. Additionally, Senso provides the safeguarding team alerts and captures evidence of misuse within the IT environment.

2. **Smoothwall** is the web filter provided by our broadband providers, Durham Council. It uses both custom and pre-defined terms to filter web activity for both staff and students. A block page is

shown if the search term or website is determined as inappropriate. For more severe content alerts, an alert is also sent to the safeguarding team.

3. Using pre-defined **Microsoft filtering** and additional custom filters, we prevent malicious emails reaching students and staff within the school. Staff and students should also use the reporting feature or submit suspicious emails that slip through the net to be reviewed. If found to be malicious in nature the email domain or the address itself is added to the block list. The IT team is then able to trace the message to alert any other recipient.

7. Acceptable use of ICT in school

All governors and staff sign an 'Acceptable Use of ICT Systems Policy agreement' annually and all students and parents sign an 'Acceptable Home-Academy agreement' detailing ICT, mobile phone and Bring Your Own Device policies. 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.

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

8. Pupils using their own electronic devices in school

Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner.

In accordance with guidance from The Department of Education (February 2024), mobile phones and other smart technology with similar functions to mobile phones (for example the ability to send and/or receive notifications or messages via mobile phone networks or the ability to record audio and/or video) are prohibited throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtimes.

The Academy has adopted the recommended 'Never used, seen or heard' policy to support the safety and welfare of our students as they travel to and from school. Phones should be switched off and stored in bags while the student is on the school site.

If a student is seen with their mobile phone in school, it will be confiscated by a member of staff and stored securely in the school office. The student will be issued with an appropriate sanction following our Behaviour for Learning Policy.

Sixth Form students are prohibited to use mobile phones on the school site apart from the Sixth Form Common Room/Building during social times. Phones should be out of sight during lessons unless otherwise instructed by a member of staff.

If a student uses their phone to take pictures during the school day on the school premises this will result in confiscation of the phone and internal isolation. Sharing of images or video taken in school will lead to a fixed term suspension.

Any mobile phones which are confiscated will be stored securely ready for collection at the end of the academy day (or at a time stipulated by the Head Teacher). The mobile phone must be collected by a parent/carer and will not be directly returned to the student.

Parents must make sure that students are able to make their way home from school without using their mobile phone.

Parents have a significant role in supporting the school's policy on prohibiting the use of mobile phones and should be encouraged to reinforce and discuss the policy at home as appropriate, including the risks associated with mobile phone use and the benefits of a mobile phone –free environment. Where parents need to contact their child during the school day, they should contact the school office. Sanctions will be given to any student using their phone throughout the day to contact parents regardless of the reason.

In accordance with the Children and Families Act 2014 and the Equality Act 2010, reasonable adjustment will be made to support students with a medical condition or disability, and this may involve the use of a mobile phone.

Examining electronic devices

Schools have the power to confiscate mobile phones or similar devices as a disciplinary penalty. The law protects staff from liability in any proceedings brought against them for any loss or damage to items they have confiscated as a sanction, providing they have acted lawfully.

Headteachers are backed by the DfE to confiscate mobile phones and similar devices for the length of time they deem proportionate.

Headteachers, or staff they authorise, have a statutory power to search a pupil or their possessions (including mobile devices) where they have reasonable grounds to suspect that the pupil is in possession of a prohibited item or image (for example an image taken on the school premises).

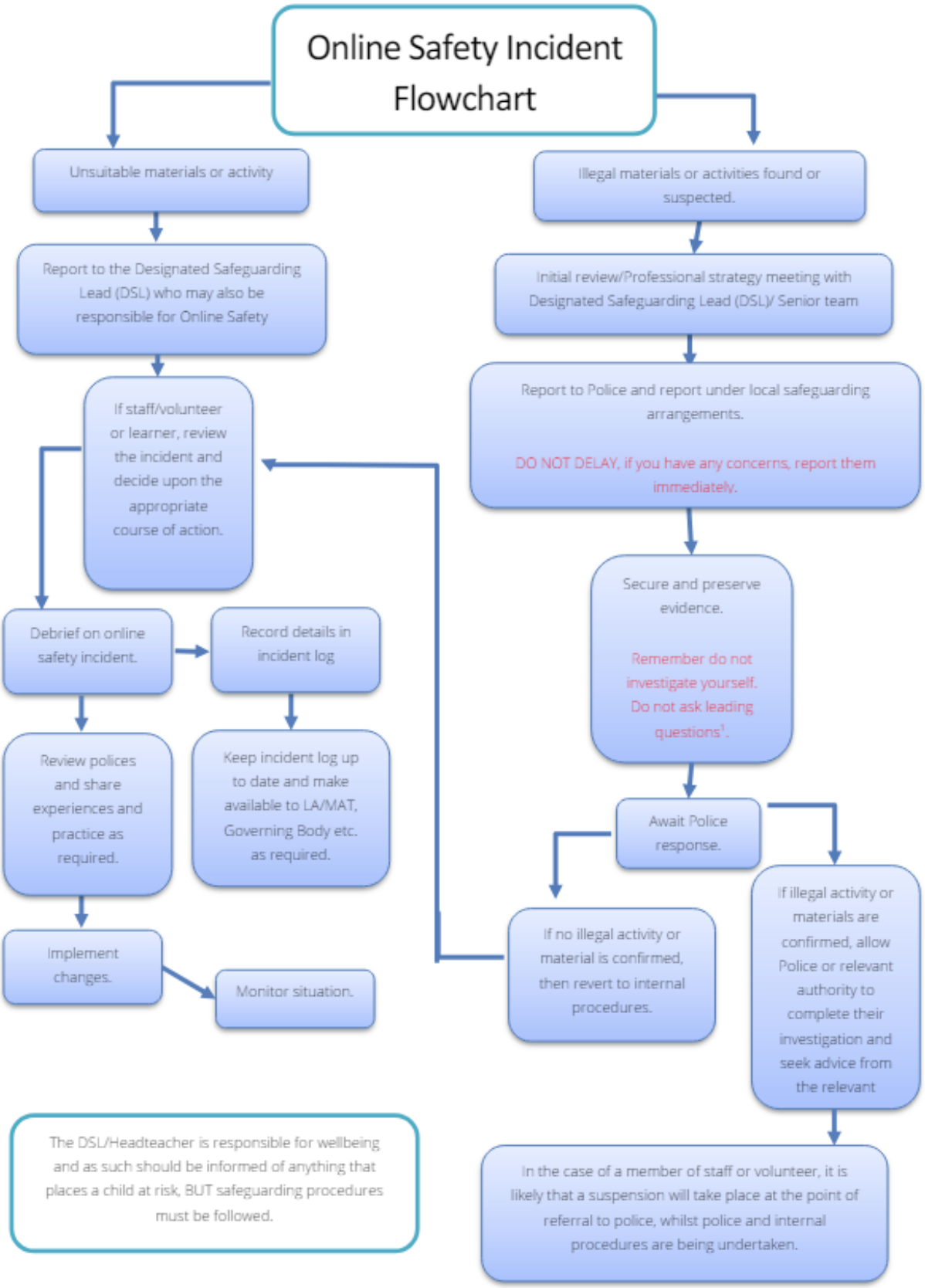
For more information, please see
https://assets.publishing.service.gov.uk/media/65cf5f2a4239310011b7b916/Mobile_phones_in_schools_guidance.pdf

9. 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 behaviour for learning 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 and staff code of conduct policies. 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:



Linked policies:

https://st-anthonys-academy.com/wp-content/uploads/2024/03/Safeguarding-and-child-protection-policy-2023-2024.pdf

https://st-anthonys-academy.com/wp-content/uploads/2024/03/STA-Behaviour-for-Learning-Policy-2023-24-Updated.pdf

https://st-anthonys-academy.com/wp-content/uploads/2023/02/Remote-learning-policy.pdf

https://st-anthonys-academy.com/wp-content/uploads/2023/05/Social-Media-Policy-Reviewed-May-2023.pdf

https://st-anthonys-academy.com/wp-content/uploads/2024/02/Acceptable-Use-of-IT-Systems-Policy-Staff.pdf

https://st-anthonys-academy.com/wp-content/uploads/2023/05/Anti-Bullying-2023.pdf