St Antony's
Roman Catholic School

Respect † Love † Integrity † Service † Resilience

Date reviewed: January 2024

Authors: Kevin Speake
Jay Haughton

E-Safety Policy

Contents

E-Safety Policy

This policy has been updated in line with the requirements of the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, to include further information on consent, data security and the responsibilities of the data protection officer (DPO). The updated policy also incorporates statutory guidance in reference to the 2023 update of Keeping Children Safe in Education.

Statement of intent

At St Antony's Roman Catholic School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

Our school 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 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

Legislation and guidance

1. This policy has due regard to all relevant legislation including, but not limited to:
    - Education Act 1996 & 2011
    - Education and Inspections Act 2006
    - Equality Act 2010
    - The General Data Protection Regulation
    - Freedom of Information Act 2000 including changes to legislation with all changes known to be in force on or before 11 January 2024
2. This policy also has regard to the following statutory guidance:
    - DfE (2023) 'Keeping children safe in education'
    - National Cyber Security Centre (published 19th October 2017) 'Cyber Security: Small Business Guide'
3. This policy will be used in conjunction with the following school policies and procedures:
    - Behaviour for Learning Policy
    - Anti-Bullying Policy
    - Data Protection Policy

- Procedure for Allegations of Abuse Against Staff
- Staff Discipline Policy
- Safeguarding Policy
- Staff Code of Conduct

Roles and responsibilities

The governing board

4. The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
5. The governing board 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.
6. The governing board will also 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.
7. The governing board 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).
8. The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
9. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 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.

The headteacher

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

The designated safeguarding lead (DSL) and their deputies

- Details of the school's designated safeguarding lead (DSL) and their deputies 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT 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 school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- 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.

The Infrastructure and Development Manager

- The Infrastructure and Development Manager is responsible for putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school 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, including terrorist and extremist material.
- Ensuring that the school's 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 school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive

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 school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.

- 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 notifying the DSL or deputies and/or the Infrastructure and Development Manager.
- Following the correct procedures by [insert school specific action here] 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 ensuring that any incidents of cyber-bullying 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, and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

Parents/carers

1. 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 school's ICT systems and internet (appendices 1 and 2)
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

https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

    Hot topics – Childnet

https://www.childnet.com/help-and-advice/parents-and-carers

    Parent resource sheet – Childnet

https://www.childnet.com/resources/parents-and-carers-resource-sheet/

Visitors and members of the community

3. Visitors and members of the community who use the school's 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.

Educating pupils about online safety

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

In KS3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

1. Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
2. 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
3. Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
4. What to do and where to get support to report material or manage issues online
5. The impact of viewing harmful content
6. That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
7. That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
8. How information and data is generated, collected, shared and used online
9. 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
10. How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
11. The safe use of social media and the internet will also be covered using additional teaching opportunities such as:
    - Assemblies
    - Tutor time resources
    - Personal Development lessons
    - Outside speakers such as:
12. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. Additional assessment may be undertaken in these instances including children from families who may have sought asylum from unstable countries to ensure they fully understand the content and are supported with the content.

Use of the internet

1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.
2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.
3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:
    - Access to illegal, harmful or inappropriate images
    - Cyber bullying
    - Access to, or loss of, personal information
    - Access to unsuitable online videos or games
    - Loss of personal images
    - Inappropriate communication with others
    - Illegal downloading of files
    - Exposure to explicit or harmful content, e.g. content involving radicalisation
    - Plagiarism and copyright infringement

- Sharing the personal information of others without the individual's consent or knowledge

Roles and responsibilities

1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.
2. The governing board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
3. The Designated Safeguarding Lead (DSL) & their deputies (DDSL) is responsible for ensuring the day-to-day e-safety in the school. The Infrastructure and Development Manager will manage the running of the systems and security of said systems, any issues discovered by the Infrastructure and Development Manager should be brought to the attention of the DSL/DDSL.
4. The Headteacher is responsible for ensuring that the Infrastructure and Development Manager and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.
5. The Headteacher and data protection officer (DPO) will ensure there is a system in place which monitors and supports the Infrastructure and Development Manager, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.
6. The Infrastructure and Development Manager will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.
7. The DSL Infrastructure and Development Manager will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
8. The DSL or their deputies will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and the Infrastructure and Development Manager will keep a log of all incidents recorded.
9. The governing board will evaluate and review this E-safety Policy on a biannual basis, considering the latest developments in ICT and the feedback from staff/pupils.
10. The DSL and their deputies will review and amend this policy with the Infrastructure and Development Manager, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
11. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
12. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.
13. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement.
14. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
15. The Headteacher through the Headteachers PA is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.
16. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

E-safety education

Educating pupils:

1. An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.
3. Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.
4. Clear guidance on the rules of internet use will be presented in all classrooms.
5. Pupils are instructed to report any suspicious use of the internet and digital devices to an adult member of staff.
6. PSHE lessons and days will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
7. The school will promote e-safety through events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

8. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
9. All staff will be educated on which sites are deemed appropriate and inappropriate.
10. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
11. The Infrastructure and Development Manager will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

12. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
13. Parents' evenings, meetings and other similar occasions may be utilised to inform parents of any e-safety related concerns.

Artificial intelligence and generative AI

1. Generative AI refers to technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. ChatGPT and Google Bard are generative artificial intelligence (AI) tools built on large language models (LLMs).

   Artificial intelligence tools such as ChatGPT and Google Bard can:

   - answer questions
   - complete written tasks
   - respond to prompts in a human-like way

   Other forms of generative AI can produce:

   - audio
   - code
   - images
   - text
   - simulations
   - videos

   AI technology is not new and we already use it in everyday life for:

   - email spam filtering
   - media recommendation systems
   - navigation apps
   - online chatbots

   Recent advances in technology mean that we can now use tools such as ChatGPT and Google Bard to produce AI-generated content. This creates opportunities and challenges for the education sector.

2. School will monitor advice sent out by the Department for Education (DfE) and the Joint Council for Qualifications (JCQ) and consider when revising the E-Safety policy.

E-safety control measures

Internet access:

1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.
2. Where a pupil is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that the pupil has consented independently.
3. A record will be kept by the headteacher of all pupils who have been granted internet access.
4. All users will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.
5. Pupils' passwords will expire every 90 days, and their activity is continuously monitored by the Infrastructure and Development Manager.
6. Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

7. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
8. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
9. The governing board will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
10. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
11. All school systems will be protected by up-to-date virus software.
12. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
13. Master users' passwords will be available to the headteacher for regular monitoring of activity.
14. Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
15. Personal use will only be monitored by the Infrastructure and Development Manager for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.
16. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

Personal devices and personal social media accounts

1. Adults must take responsibility for their personal telephones and any personal electronic devices and must keep their personal telephone numbers, login details, passwords, pin details and personal email addresses private and secure.
2. Where there is a need to contact pupils or parents the school's email address and/or telephone should be used. Adults must not use their personal telephones or email accounts for these purposes.
3. Adults must understand who is allowed to view the content on their social media pages of any websites they use and how to restrict access to certain groups of people. Appropriate privacy settings are vital.
4. Adults must not request, or respond to a request for any personal information from or about a pupil at the school.
5. Adults must not engage in conversations about pupils with their parents or carers or with any other person by any form of social networking or social media unless they have the express permission of the Headteacher to do so.
6. Adults must only use the official school email for communicating with pupils or to enable pupils to communicate with each other using authorised and previously agreed protocols. Any communications with pupils (including by email, telephone or text communications) outside of agreed protocols will be treated as a very serious conduct matter and may lead to disciplinary action being taken under the school's Disciplinary Policy which, in serious cases may lead to dismissal without notice. It may also lead to a criminal investigation.
7. Adults must never connect to or have any contact with a pupil at the school on any social networking site. The only exceptions to this rule are where the pupil is a member of the adult's family provided agreed protocols are followed and the family relationship has been identified to and acknowledged by the Headteacher.
8. In cases where a pupil is a family member, adults must be aware that if the family relationship has not been identified and acknowledged by the school, contact through social networking or social media will be a breach of this policy (and therefore will be treated as a serious conduct issue). Adults must be clear that such contact could also be misconstrued as being part of a grooming process. Since family relationships can be easily identified and recognised, adults must notify the Headteacher of any family relationship with a pupil so that the position can be formally acknowledged, discussed and recorded.

9. Adults must be cautious about any form of social networking contact with former pupils, parents/carers of pupils, particularly where siblings or other relatives continue to attend the school or may attend the school in future.
10. Adults must be mindful at all times of the boundaries between their work and personal life in accordance with the Key Principles detailed in this policy, and in the Guidance for Safer Working Practices for Adults who work with Children and Young People in Education 2019.
11. Adults must also be cautious when inviting work colleagues to be friends on social networking sites. Social networking sites can blur the boundaries between work and personal lives and it may be difficult to maintain professional relationships.
12. Adults must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring them or the school and the wider school community into disrepute or which could be interpreted as reflecting negatively on their professionalism.
13. Adults must not represent their personal views on any social media forum as being in any way linked to the school or being the views of the school.
14. Photographs, videos or any other types of images of pupils and their families or images depicting staff members or where the school can be identified must not be published on social media.
15. Where social networking and other web-based sites have fields in the user profile relating to job title or information, all adults should not put any information onto the site which could identify the school or their role at the school (particularly teachers and teaching assistants where pupils maybe identifiable). In some circumstances the provision of such information could damage the reputation of the school and/or the relevant profession.
16. Teachers must at all times be mindful of the Teachers' Standards applicable to their profession and act in accordance with those standards. The Teacher Standards make clear that a teacher must uphold public trust in the profession and maintain high standards of ethics and behaviour both within and outside of school, by ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law. Any breach of the Teacher Standards will be considered a matter of misconduct and may lead to disciplinary action being taken under the school's Disciplinary Policy which, in serious cases may lead to dismissal without notice.
17. Adults must devote the whole of their time and attention to their duties during working hours. Personal use of the internet is not permitted during working hours and it is strongly recommended that 3G/4G access is switched off during working hours. Exceptions to this must be agreed by a member of the school leadership team (SLT) and reviewed daily. Any breach of this provision will be regarded as a conduct matter and disciplinary action taken as appropriate. Include when mobile phones and social media sites can be use during school hours i.e. in the staff room during the lunchtime period] Staff personal mobile phones are to only be used in the staff room during breaks and lunchtimes. They are only ever to be used in a classroom setting to photograph work for assessment or celebration purposes.
18. Confidentiality issues must be considered at all times in relation to social networking and the use of social media. All employees are bound by a common law duty of fidelity. There are also other laws which protect the school's confidential information which adults working in school may have access to during the course of their work. Confidential information includes but is not limited to person identifiable information, for example pupil and employee records, information protected by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018 and information provided by the school in the expectation of confidence including information about the school, pupils and the families of pupils, the school's staffing or business plans, and any other commercially or politically sensitive information.
19. Adults must ensure that they do not provide, publish share or otherwise disclose any confidential information about themselves or about the school and the wider school community in breach of their duty of fidelity or in breach of other laws relating to confidentiality and privacy including the Human Rights Act 1998, the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018.

20. Adults must ensure they understand their obligations under the Equality Act 2010 and under the school's Equality Policy. Breaches of the Equality Act 2010 or the school's Equality Policy through the use of social networking or social media will be considered a serious conduct matter which may lead to disciplinary action being taken under the school's Disciplinary Policy which, in serious cases may lead to dismissal without notice. Adults should also be aware that they could be held personally liable for their own discriminatory actions under the Equality Act 2010. If, for example an adult were to harass a co-worker online or engage in a discriminatory act in relation to one of the protected characteristics under the Equality Act 2010, this may result in legal action being taken against them.
21. Adults should also be aware that there are other laws relating to libel, defamation, harassment and copyright which may apply to information, published or posted by them on social media and which could lead to legal action being taken against them. In addition, this will be considered as a serious conduct matter and may lead to disciplinary action being taken in line with the school's Disciplinary Policy, which may lead to dismissal without notice.
22. All concerns about communications, social contact or social media/social networking issues must be raised with the Headteacher immediately.

Access to inappropriate images

1. There are no circumstances which justify adults possessing or sharing indecent images of children whether in working time or in an adult's personal time. Adults who access and/or possess links to such material or websites will be viewed as a significant and potential threat of harm to children or vulnerable adults. Appropriate action will be taken against the adult concerned in these circumstances which, for the avoidance of doubt, could include action under the school's Safeguarding Policy (which could lead to police and Local Authority involvement) and disciplinary action under the school's Disciplinary Policy (which could result in dismissal without notice on the grounds of gross misconduct). Where indecent images of children are found by any adult, the Headteacher must be informed immediately.
2. Adults must not use equipment belonging to the school to access pornography or adult or explicit material of any kind. Personal equipment containing these images or links to them must not be brought into school. If any adult uses school equipment or personal equipment in school to access pornography or links to it, this will raise serious concerns about the suitability of the adult concerned to work with children. This will lead to an investigation under the school's Disciplinary Policy and may lead to disciplinary action and any other action considered appropriate in the circumstances.
3. Adults must ensure that pupils are not exposed to any inappropriate information, images or web links. The school will endeavour to ensure that internet equipment used by pupils has the appropriate controls with regards to access. Any concerns or potential issues identified by any adult must be reported immediately to the Headteacher.
4. Where any form of unsuitable material is found, which may not be illegal but which could or does raise concerns about an adult working in school, the Headteacher should be informed immediately. The Headteacher may take HR or legal advice on the appropriate way forward.

Examining electronic devices

1. 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

2. Members of staff should consult with a member of SLT before undertaking a search of a phone or mobile device. If a member of SLT is unavailable, the device should be confiscated until the search has been authorised. In any event of a search where possible, parents should be informed.
3. Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
    - 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
4. 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 especially if there is a safeguarding risk.
5. When deciding whether there is a 'good reason' to examine data or files on an electronic device ,relevant staff 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
    - Knowingly or unknowingly put a pupil or member of staff at risk
6. If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / headteacher / 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.
7. 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/carer refuses to delete the material themselves
8. 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 deputy) 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
9. Any searching of pupils will be carried out in line with the schools' search policy which takes guidance from the DfE's latest guidance on searching, screening and confiscation.

Email:

1. Pupils and staff will be given approved email accounts and are only able to use these accounts.
2. The use of personal email accounts to send and receive personal data or information is prohibited.
3. No sensitive personal data shall be sent to any other pupils, staff or third parties via email without first being encrypted and password protected.

4. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
5. Staff members are aware that their email messages are not monitored.
6. Staff to inform the DSL or their deputies along with the Infrastructure and Development Manager if they suspect their email has been accessed by a third party.
7. Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
8. Chain letters, spam and all other emails from unknown sources will be deleted without opening.
9. The DSL or their deputies along with the Head of Computing will, at the start of each school year, hold an assembly explaining what a phishing email might look like – this assembly will include information on the following:
10. Determining whether or not an email address is legitimate
11. Knowing the types of address a phishing email could use
12. Asking "does it urge the recipient to act immediately?"
13. Checking the spelling and grammar
14. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The Infrastructure and Development Manager supported by the DSL and their deputies if required will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

1. Social media development on behalf of the school is conducted by the Headteacher's PA.
2. Access to social networking sites will be filtered as appropriate.
3. Staff access to the schools' official social media channels to be managed by the Headteacher's PA.
4. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
5. Pupils are regularly educated on the implications of posting personal data online outside of the school.
6. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
7. Staff should not communicate with pupils over social networking sites and are reminded to alter their privacy settings.
8. Staff are not permitted to publish comments about the school which may affect its reputation.
9. Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the Headteacher prior to accessing the social media site.

Published content on the school website:

1. The Headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
2. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
3. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until authorisation from parents has been received.
4. Pupils are not permitted to take or publish photos of others without permission from the individual.

5. Staff are able to take pictures though they will not take pictures using their personal equipment.
6. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.
7. The DSL and their deputies will manage the list of children who do not have permission to have photographs taken.
8. Staff on school trips/events will be made aware of the students without photograph consent prior to leaving on the trip.

Mobile devices and hand-held computers:

1. The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
2. Pupils are only permitted to access the school's Wi-Fi system during Study hall scheduled by the head of year and set up by the Infrastructure and Development Manager, the use of student mobile devices and hand-held computers must be supervised by the study hall staff member.
3. Mobile devices are not permitted to be used during school hours by pupils or members of staff with the exception of Authenticating password for multifactor authentication.
4. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the Infrastructure and Development Manager where it is justifiable to do so and the justification outweighs the need for privacy.
5. The sending of inappropriate messages or images from mobile devices is prohibited.
6. Personal mobile devices will not be used to take images or videos of pupils or staff.
7. No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks. Infrastructure and Development Manager will inform pupils and staff members of this rule before they can use school-owned devices away from the premises.
8. The DPO will, in collaboration with the Infrastructure and Development Manager, ensure all school-owned devices are password protected – these passwords will be changed after each use to ensure their security.
9. All mobile devices and hand-held computers will be fitted with tracking software to ensure they can be retrieved if lost or stolen if feasible.
10. To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed where feasible.
11. The Infrastructure and Development Manager will review all mobile devices and hand-held computers on a monthly basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.
12. [New] The Infrastructure and Development Manager will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician or the Infrastructure and Development Manager.
13. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Mobile internet devices provided by school (portable WiFi routers)

1. Any mobile Wi-Fi devices given to students/parents to enable internet access at home remain the property of school unless otherwise stated.

2. Any Sim-Cards and internet access through these devices must be filtered and monitored by the parent through the device used to view the content (phone/tablet/PC)
3. School cannot be responsible for filtering and monitoring on personal devices.

Network security:

1. Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.
2. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
3. Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.
4. Passwords will expire after 60 days to ensure maximum security for pupil and staff accounts.
5. Passwords should be stored using non-reversible encryption.
6. The Infrastructure and Development Manager will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.
7. Important folders, e.g. those including pupils' medical records, will be password protected to ensure their security – the Infrastructure and Development Manager, school nurse and other designated individual(s) will be the only people who have access to this password.
8. Students found to have breached network security and/or pose a threat to network security can have their access revoked and may be required to complete computer work on an isolated (off network) device.
9. Staff must lock computers they are logged into when left unattended.
10. Staff must not log into a computer to allow a child access to the internet or network.
11. Staff must not use 'incognito' or private browsing whilst on school devices.
12. Use of virtual private network (VPN) and other services to bypass security is not allowed by either staff or students, any bypassing of security will be investigated by the DSL or their deputies.

Virus management:

1. Technical security features, such as virus software, are kept up-to-date and managed by the Infrastructure and Development Manager.
2. The Infrastructure and Development Manager will ensure that the filtering of websites and downloads is up-to-date and monitored.
3. Firewalls will be switched on at all times – The Infrastructure and Development Manager will review these on a regular basis to ensure they are running correctly and to carry out any required updates.
4. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's Data Security Breach Prevention and Management Plan.
5. Staff members will report all malware and virus attacks to the Infrastructure and Development Manager and DPO immediately.
6. Use of memory sticks, portable HDD/SSD and other portable storage devices are not allowed and their use has been disabled on school systems by default.
7. Information required to be added to the school network by portable storage device (ie assembly presentations from external agencies) must be given directly to the Infrastructure and Development Manager to copy onto the school's network.

Cyber bullying

1. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.
2. The school recognises that both staff and pupils may experience cyber bullying and is committed to responding appropriately to instances that should occur.
3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our Anti-Bullying and Harassment Policy and Cyber Bullying Policy.
7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator of Trafford LA of the action taken against a pupil.

Reporting misuse

1. St Antony's Roman Catholic School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.
2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

3. Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
4. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher using a complaints form.
5. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet will have a letter sent to their parents explaining the reason for suspending their internet use.
6. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.
7. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff:

8. Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a complaints form.
9. The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy and may decide to take disciplinary action against the member of staff.
10. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Use of illegal material:

11. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.
12. Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
13. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.
14. [New] Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

Training

All 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 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, threatening, 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

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

Staff will receive training on the school filtering and monitoring systems which includes:

- Their responsibility in preventing breaches of filtering and monitoring systems
- who to report filtering and monitoring breaches to
- How to set classwork and tasks for pupils which takes into account online safety

Monitoring and review

1. The e-safety committee will evaluate and review this E-safety Policy on a termly basis, taking into account the school's e-safety calendar, the latest developments in ICT and feedback from staff/pupils.

2. This policy will also be reviewed on an annual basis by the governing board; any changes made to this policy will be communicated to all members of staff.
3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.