St Anthony's Catholic Primary School

An Academy within The Catholic Academy Trust in South Hampshire

'Children in our heart, Christ at the centre'
'We love, we learn and we live'

Name of Policy	Safe Use of Technology Policy
Reference Number	
Date of e-signoff	October 2026
Headteacher	Katrina Straker
Chair of Standards & Admissions Sub-Committee	Anne Taylor
Date for review	October 2027

Safe Use of Technology Policy

St Anthony's Catholic Primary School

An Academy within The Catholic Academy Trust in South Hampshire

'Children in our heart, Christ at the centre'
'We love, we learn and we live'

The St Anthony's mission statement is 'Children in our heart, Christ at the centre. We love, we learn and we live.' To live out this mission, we are guided and led by our Catholic ethos that places the Catholic Social Teaching principles of Human Dignity and the Common Good at the heart of our school. We recognise that each of us is unique and loved by God and we are called to lead by example, as Christ did, to show respect and love to every person because each of us is made in the image of God.

Contents

1. Introduction and aims 4
2. Relevant legislation and guidance 4
3. Definitions 5
4. Unacceptable use 5
    4.1 Exceptions from unacceptable use 5
    4.2 Sanctions 5
5. Roles and responsibilities 5
    5.1 The governing board 5
    5.2 The Headteacher 6
    5.3 The designated safeguarding lead (DSL) 6
    5.4 Headteacher and Office Manager 6
    5.5 All staff and volunteers 6
    5.6 Parents/carers 6
6. Staff use of technology 6
    6.1 Access 7
    6.2 Use of phones and email 7
    6.3 Personal use 7
    6.4 Personal social media accounts 7
    6.5 Remote access 7
    6.6 School social media accounts 8
    6.7 Monitoring and filtering of the school network and use of ICT facilities 8
    6.8 Device security 8
    6.9 Maintaining cyber security 8
7. Pupil use of technology 8
    7.1 Access to ICT facilities 8
    7.2 Pupils using mobile devices in school 8
    7.3 Unacceptable use of ICT and the internet outside of school 9
8. Parents and carers 9
    8.1 Access to ICT facilities and materials 9
    8.2 Communicating with or about the school online 9

8.3 Communicating with parents/carers about pupil activity 10
9. Educating about online safety 10
9.1 Educating pupils about online safety 10
9.2 Educating parents/carers about online safety 10
10. Cyber-bullying 10
10.1 Definition 10
10.2 Prevention and response 10
10.3 Artificial intelligence (AI) 11
11. Data security 11
12. Protection from cyber attacks 11
12.1 Types of threats 11
12.2 Mitigation measures 11
12.3 Critical incident plan 12
13. Internet access and filtering 12
14. Artificial intelligence (AI) 12
14.1 Generative AI systems 12
14.2 Staff use of AI 13
14.3 Pupil use of AI 13
14.4 Monitoring and review 13
15. Use of mobile phones and personal devices 13
15.1 Use of personal mobile phones by staff 13
15.2 Use of work phones by staff 14
15.3 Use of mobile phones and other personal devices by pupils 14
15.4 Sanctions 15
15.5 Safeguarding 15
15.6 Use of personal devices by parents/carers, volunteers and visitors 15
16. Social media 15
16.1 Official school social media 15
16.2 Code of Conduct 16
16.3 Administration 16
17. Response to issues of misuse 16
18. Training 16
19. Related policies 16
Appendix 1: Acceptable use agreement for pupils 17
Key Stage 1 guidance (Year 1 & 2): 17
Lower Key Stage 2 guidance (Years 3 & 4): 17
Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors 20
Appendix 3: Acceptable use agreement for parents and carers 21
Appendix 4: Online safety training needs – self-audit for staff 22
Appendix 5: Glossary of cyber security terminology 23
Appendix 6: The ethical framework for AI in education 25
European Commission: 25
UNESCO: 25

1. Introduction and aims

Information and Communications Technology (ICT) is integral to how our school operates and is a critical resource for pupils, staff, governors, volunteers and visitors. However, it poses risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines for ICT use across the school community
- Establish clear expectations for online engagement
- Support our data protection and safeguarding policies
- Teach pupils safe and effective internet use
- Identify and support pupils at greater risk online
- Establish clear incident response mechanisms
- Prevent disruption through ICT misuse
- Minimise cyber security risks

This policy covers all users of our ICT facilities. Breaches may be dealt with under our Disciplinary Policy or Staff Code of Conduct.

The 4 key categories of online risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – illegal, inappropriate or harmful material
- **Contact** – harmful online interaction with others
- **Conduct** – personal behaviour that causes harm
- **Commerce** – online gambling, scams and inappropriate advertising

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Data (Use and Access) Act 2025
- Children's Wellbeing and Schools Act 2026 (section 36)
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 1996 (as amended)
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Equality Act 2010
- Education and Training (Welfare of Children) Act 2021
- Keeping Children Safe in Education 2026
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes
- Meeting digital and technology standards in schools and colleges
- DfE guidance on Generative artificial intelligence (AI) in education
- DfE mobile phone guidance
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff

The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

3. Definitions

- **ICT facilities**: All technology including computers, tablets, phones, software, websites and future devices
- **Users**: Anyone authorised to use school ICT
- **Personal use**: Non-work-related activity
- **Social media**: Technologies enabling communication and information sharing
- **Generative AI**: AI systems generating new content (text, images, audio, video)

See Appendix 5 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Infringing intellectual property rights or copyright
- Bullying, harassment or unlawful discrimination
- Illegal conduct or advocacy
- Online gambling, scams or phishing
- Accessing, creating or sharing pornographic, offensive or harmful material
- Making or sharing nudes or semi-nudes (including AI-generated deepfakes) Online safety: requirements and guidance (The Key Leaders)
- Defaming the school or risking its reputation
- Sharing confidential information
- Unauthorised network connections or software installation
- Attempting to access restricted areas or password-protected information
- Intentional damage to ICT facilities
- Data breaches
- Using AI to complete homework presented as pupil's own work (unless permitted by teacher)

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use her professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

The Headteacher may grant exemptions in writing via office@saint-anthonysfareham.co.uk.

4.2 Sanctions

Breaches will result in disciplinary action in line with school policies.

5. Roles and responsibilities

5.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will:

- Ensure staff understand expectations around filtering and monitoring Online safety: requirements and guidance
- Review the DfE filtering and monitoring standards and discuss with IT staff how to meet them Online safety: requirements and guidance
- Review filtering and monitoring effectiveness at least annually Online safety: requirements and guidance
- Conduct annual cyber security reviews
- Ensure the school meets DfE Cyber Security Standards

The governor who oversees online safety is the Safeguarding Governor.

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 and the internet (Appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding

5.2 The Headteacher
The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school in line with the actions listed in 5.1.

5.3 The designated safeguarding lead (DSL)
The DSL (who is also the Headteacher at our school) takes lead responsibility for online safety in school, in particular:
- Ensuring staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually
- Taking the lead on understanding the filtering and monitoring systems and processes in place
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents, including cyber-bullying, are logged and dealt with appropriately
- Liaising with other agencies and/or external services if necessary
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually

5.4 Headteacher and Office Manager
The Headteacher and Office Manager will work with the school's IT Support Partner (currently Alphascan) to:
- Implement filtering and monitoring systems
- Ensure ICT security
- Block dangerous sites
- Manage access to ICT facilities

5.5 All staff and volunteers
All staff, including contractors and agency staff, and volunteers must:
- Implement this policy consistently
- Follow the terms on acceptable use (Appendix 2)
- Ensure that pupils follow the school's terms on acceptable use (Appendix 1)
- Know the DSL is responsible for filtering and monitoring systems
- Report system failures immediately
- Seek authorisation before bypassing filtering systems
- Work with the DSL and/or the Deputy DSLs to ensure that any online safety incidents, including cyber-bullying, are logged and dealt with appropriately
- Respond appropriately to all reports and concerns about sexual violence and/or harassment or harmful behaviour, both online and offline

5.6 Parents/carers
Parents/carers are expected to:
- Support their child in understanding acceptable use (Appendix 1)
- Comply with the acceptable use agreement through the Home School Agreement (Appendix 3)

6. Staff use of technology

6.1 Access
The school's Office Manager (OM), with the support of the school's IT Support Partner (currently, Alphascan), manages access to the school's ICT facilities for school staff.

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

6.2 Use of phones and email
The school provides each member of staff with an email address. This email account should be used for work purposes only.
Staff must enable multi-factor authentication on their email account(s).
Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.
Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract or generally bring the reputation of the school in to disrepute.
Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted.
Staff should follow data breach procedures if emails are sent or received in error.
Staff must not give their personal phone number(s) to parents/carers or pupils for school purposes save in exceptional circumstances approved by the Headteacher (for example co-ordinating medical treatment for a child on a school trip, or monitoring a child's medical needs via a shared medical app). Staff must use phones provided by the school to conduct all work-related business e.g. school trips (see Section 15).

6.3 Personal use
Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions. This permission must not be overused or abused. The OM or Headteacher may withdraw or restrict this permission at any time.
Personal use is permitted provided that such use:
- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their work

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials.
Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

6.4 Personal social media accounts
Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.
When using social media, staff **must not**:
- Use personal accounts for school business
- Accept 'friend requests' from pupils past or present
- Make posts that unlawfully disclose confidential or personal information, harass or discriminate against others, or reasonably undermine safeguarding or professional duties. Nothing in this policy prevents lawful trade-union activity, protected disclosures, reporting wrongdoing to an appropriate body, or the lawful exercise of freedom of expression.
- Post images of pupils
- Link their social media profile to their work email account
- Use personal social media during timetabled teaching time

6.5 Remote access
Staff may access school systems remotely via the VPN managed by the IT Support Partner (currently Alphascan), following the same rules as on-site use.

6.6 School social media accounts

The school has its own Facebook account. Only authorised staff may access the school's Facebook account.

6.7 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children, the school will

- Undertake filtering and monitoring only for specified, lawful and necessary purposes
- Identify and document the lawful basis
- Complete and keep under review a data protection impact assessment where required
- Provide clear privacy information to pupils, staff and other users
- Restrict access to monitoring records
- Retain them only for a defined period
- Ensure that monitoring is proportionate and no more intrusive than necessary.

6.8 Device security

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping accounts and devices protected by the school's approved authentication controls. Passwords must meet the minimum length set by the school's identity system, must not be commonly used or compromised, and must not be reused across work and personal accounts. Multi-factor authentication must be enabled where available. Routine password expiry or forced periodic changes will not be required unless there is evidence or suspicion that an account has been compromised.
- Ensuring hard drives are encrypted
- Keeping systems updated
- Locking devices when unattended
- Never sharing passwords or allowing family/friends to use school devices
- Installing anti-virus software
- Reporting stolen equipment immediately

6.9 Maintaining cyber security

Emails often host scams and malicious software (e.g. malware or ransomware). To avoid virus infection or data theft, staff must:

- Avoid opening attachments or clicking on links when the content is not adequately explained
- Be suspicious of unsolicited or misleading email subject lines
- Check the email address of the sender to ensure that they are legitimate
- Look for inconsistencies or 'giveaways', for example poor grammar and spelling mistakes
- If suspicious of an email received, refer the email to a member of the SLT, the School Office Manager and report it to the IT Support Partner (currently Alphascan).

7. Pupil use of technology

7.1 Access to ICT facilities

- Laptops are available to pupils only under the supervision of staff
- Pupils will be provided with an account to save their work on a shared 'community' drive but this should only be accessed under the supervision of staff using a device from the school's laptop trolley

7.2 Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day, in line with the acceptable use agreement (see Appendix 1).

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.

7.3 Unacceptable use of ICT and the internet outside of school

The school may impose a sanction for online behaviour outside school only where the behaviour policy permits this and where it is reasonable for the school to regulate the conduct, including conduct during a school-organised or school-related activity, while travelling to or from school, when wearing school uniform or otherwise identifiable as a pupil at the school, or conduct that could have repercussions for the orderly running of the school, poses a threat to another pupil or member of the public#, or could adversely affect the school's reputation. Any response will be lawful, reasonable, proportionate and safeguarding-led.
Examples of unacceptable use include:

- Using ICT or the internet to infringe intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Making or sharing of nudes or semi-nudes
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

In situations when the activity has taken place outside school hours, the Headteacher or a member of the Senior Leadership Team will discuss what has taken place with the pupil's parent/guardian unless there is a safeguarding concern. If there is a safeguarding concern, the Headteacher (who is also the Designated Safeguarding Officer) will follow the school's safeguarding procedures in line with the Safeguarding and/or Child Protection Policies.

8. Parents and carers

8.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.
However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access at the Headteacher's discretion. Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

8.2 Communicating with or about the school online

Parents/carers play a vital role in helping model appropriate online behaviour for their children.
We ask parents/carers to comply with the agreement in Appendix 3, when they consent to the school's 'Home school agreement'.

When communicating with the school or using private/independent channels to talk about the school, parents and carers should:

- Be respectful towards, and about, members of staff and the school at all times
- Be respectful of, and about, other parents/carers and other pupils and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

Parents/carers **should not** use social media to:

- Complain about individual members of staff, other parents/carers or pupils
- Complain about the school
- Make inappropriate comments about members of staff, other parents/carers or pupils
- Draw attention to, or discuss, behaviour incidents
- Post images of children other than their own

We expect parents/carers to follow these guidelines when using class WhatsApp groups.

8.3 Communicating with parents/carers about pupil activity
The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.
In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. Educating about online safety

9.1 Educating pupils about online safety
Pupils will be taught about online safety as part of the curriculum, with teaching adapted for vulnerable children and those with SEND where necessary. The school uses ProjectEvolve (a scheme of work) to teach about online safety at the start of every computing lesson.

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:
- People behave differently online
- Online relationships require the same respect as face-to-face
- Rules for keeping safe online and how to recognise risks
- How to critically consider online friendships
- How information is shared online

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

9.2 Educating parents/carers about online safety
The school will raise awareness through letters, newsletters, the website and parents' evenings, covering:
- Filtering and monitoring systems
- What children are asked to do online

If parents/carers have queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher, who is also the DSL.

10. Cyber-bullying

10.1 Definition
Cyber-bullying takes place online. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

10.2 Prevention and response
We will:
- Ensure pupils understand cyber-bullying and how to report it
- Discuss it during Friendship Week
- Cover it in Personal Development Learning (PDL) lessons
- Train all staff, governors and volunteers so we are ready to support pupils who may be affected

- Send information to parents/carers so they are able to spot the signs and support children
- Follow our behaviour policy processes for incidents

10.3 Artificial intelligence (AI)

AI can be used to bully others through 'deepfakes' – AI-created images, audio or video hoaxes that look real, including deepfake pornography.
Any AI use for bullying will be treated under our behaviour policy.
For more detail on how the school interacts with AI, see Section 14.

11. Data security

The school takes steps to protect the security of its computing resources, data and user accounts by implementing:

- Firewalls and security features
- Multi-factor authentication
- Anti-malware software
- Strong password requirements (see Section 6.8)
- Regular software updates
- Appropriate encryption
- Access controls

The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

12. Protection from cyber attacks

The glossary (Appendix 5) aims to support a more detailed understanding of cyber security terminology.

12.1 Types of threats

Cyber incidents and attacks can have significant operational and financial implications upon schools. These are usually deliberate and unauthorised attempts to access or damage data, or extort money from the school and can lead to damaging outcomes.
Threats include:

- Malware (malicious software) and ransomware (malware that locks victims out of their data/systems and only allows access once ransom has been paid)
- Phishing (emails purporting to come from a known source to extract sensitive information from a recipient)
- Hacktivism (hacktivists take over public websites or social media accounts to raise the profile of a particular cause)
- Insider threats (intentional or unintentional release of sensitive data into the public domain)
- Zero-day threats (a cyber-attack that occurs on the same day that a weakness is discovered in software and is exploited before a solution becomes available from its creator)
- Physical threats (increasing reliance on digital services brings an increased vulnerability in the event of a flood, fire, power-cut or other disaster, natural or otherwise)

12.2 Mitigation measures

The school will work closely with our IT Support Partner (currently, Alphascan), and will:

- Provide annual staff training on cyber security
- Not engage with ransom requests
- Implement proportionate, multi-layered, regularly reviewed controls
- Back up data daily (on-site and off-site)
- Use VPN for remote access
- Enable multi-factor authentication
- Conduct regular access reviews
- Maintain firewalls
- Check supply chain security

- Review and test incident response plans annually

12.3 Critical incident plan

This should be read in conjunction with the school's Business Continuity Plan.
Steps include:

1. **Notify key personnel:** notify the Headteacher, DSL, IT support provider (currently, Alphascan), Chair of Governors and the school's formally appointed Data Protection Officer. The DPO must be able to perform the role independently and must not hold duties that create a conflict of interests in determining the purposes and means of processing personal data.
2. **Identify and assess the incident**: collect evidence (logs, screenshots etc.) for analysis
3. **Contain the incident: i**solate affected systems, disable compromised accounts and change passwords
4. **Notify relevant parties:** promptly Assess whether personal data has been breached. Notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of a breach that is likely to result in a risk to individuals' rights and freedoms; notify affected individuals without undue delay whether breach is likely to result in a high risk. Contact the police, Action Fraud the National Cyber Security Centre, the local authority and other agencies where appropriate and keep the required breach record even where no ICO notification is made.
5. **Communicate with families and authorities**
6. **Investigate and recover:** restore systems/data securely and assess any data breaches to determine the impact on personal information
7. **Review and report incident:** document the incident details, responses and lessons learned
8. **Provide support for affected individuals**
9. **Update policies:** update cyber security policies and incident response protocols and implement further training/awareness campaigns based on findings

13. Internet access and filtering

The school uses Fortigate filtering through Alphascan and checks this at least twice yearly during safeguarding audits.
WiFi access is limited to school devices. Guest WiFi requires Headteacher authorisation.
The school uses Senso to monitor activity on school devices. Staff supervising pupils online must remain vigilant about what pupils search and view, as filters are not fool proof. Human oversight is essential.
In every computing lesson, pupils are taught about internet safety and this includes how to flag any content that makes them feel uncomfortable to a trusted adult (see Section 9).

14. Artificial intelligence (AI)

The school is chiefly concerned with cultivating human intelligence but recognises that AI can be used as an educational tool. AI can also support and reduce workload for staff across the school.
Our use of AI should always be in line with the following principles:

- The education, wellbeing and safety of our pupils must always be prioritised
- Pupils and staff must uphold high standards of academic rigour and academic integrity
- In a world full of disinformation, all must be alert to the difference between truth and falsehood, between what is genuine and what is artificial
- AI must be used safely, ethically and within the limits permitted by regulation, statutory requirements and agreed educational best practice

14.1 Generative AI systems

The school encourages staff to use Microsoft Copilot, signed in with school Microsoft 365 accounts, for increased privacy and security. Staff must use only school-approved AI tools and must not enter personal data, special-category data, confidential information or copyrighted material unless the proposed use has been approved following consultation with the Headteacher (who is the DPO), a lawful basis and any required condition have been identified, an appropriate data protection impact assessment has been completed, and affected individuals have been given suitable privacy information. A first name may still be personal data when a person can be identified from the context and must not be treated as automatically anonymous. Staff must be trained to spot and correct errors or bias in AI outputs.

Other tools (ChatGPT, Suno, etc.) require permission from the Senior Leadership Team before use.

14.2 Staff use of AI
Staff are encouraged to use AI for:
Enhancing teaching: simplifying texts, creating images, generating questions, creating WAGOLLs
Reducing workload: lesson planning, generating spelling tests, creating assessments, drafting communications, summarising documents
Staff must seek permission from the Senior Leadership Team before using AI for other tasks/purposes.

14.3 Pupil use of AI
Our Computing scheme of work, iCompute, includes three units of study to teach children about AI in Years 1, 4 and 6:
Year 1: pupils are introduced to AI and learn that AI systems are all around them and part of everyday life. They begin to learn that machines can learn and that they are trained by people. They start to explore AI's potential and its limitations.
Year 4: pupils are introduced to Machine Learning and AI. They explore the machine learning process and discover how AI systems are trained and learn from examples given to them by humans. They learn about the potential of AI and its limitations. They train machine learning models and create their own AI systems.
Year 6: pupils explore what makes intelligence artificial, the benefits and drawbacks and train their own models to produce AI applications using Scratch.

Pupils must:
- Not use AI to create harmful content
- Never pass off AI work as their own
- Only use AI under teacher guidance
- Reference any AI use clearly (eg homework projects)

14.4 Monitoring and review
As new products/software appear, these should be reviewed by the Leadership team in the first instance before they are used for educational (or other) purposes by staff or pupils.

15. Use of mobile phones and personal devices
The Department for Education's statutory guidance "Mobile phones in schools", Which schools should follow from 1 September 2026, states that schools should be mobile phone-free environments by default and should prohibit the use of mobile phones and other smart technology with similar functionality throughout the school day, subject only to limited, reasonable exceptions (eg medical reasons). This policy will be implemented consistently with the behaviour policy, safeguarding duties, the Equality Act 2010 and the duty to make reasonable adjustments.

15.1 Use of personal mobile phones by staff
Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone during the school day during contact time. Use of personal phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).
There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time, for personal reasons. For instance (this list is non-exhaustive):
- For emergency contact by their child, or their child's school or in the case of acutely ill dependents or family members
- For urgent contact by a medical professional
- To monitor a medical condition whether their own or a pupil's (e.g. use of a mobile phone to monitor glucose levels before administering insulin or avoiding a hypoglycaemic episode).

The Headteacher will decide on a case-by-case basis whether to allow for special arrangements and staff must seek permission before leaving their phone on in the presence of pupils. If special arrangements are

not deemed necessary, school staff can use the school office number 01489 579100 as a point of emergency contact.

Staff must not use personal mobile phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil. If it's necessary to take photos or recordings as part of a lesson / school trip / activity, this must be done using school equipment.
In some circumstances, it may be appropriate for staff to use personal mobile phones or a similar device during the school day in front of pupils for work. Such circumstances may include, but are not limited to:

- Use of multi-factor authentication
- Supervising off-site trips including residential visits.

In these circumstances, staff will use their mobile phones in an appropriate and professional manner in line with our staff Code of Conduct. Where possible, contact with parents will be made via the school office.

Permission must be sought before connecting personal devices to the school's network. The Headteacher may authorise a guest device (any device which is not school owned or on the school asset list) to connect to the school's Guest Wifi. Where A personal device connects to school systems, the school may monitor network and security data only to the extent necessary and proportionate for safeguarding, cybersecurity and system administration. The school will not access content stored locally on a personal device unless lawful authority exists and the action is necessary, proportionate and authorised. Users will be told what is monitored, why, the lawful basis, who may access the information and how long it is retained.

The school is not responsible for the loss, or theft of, or damage to a personal device or storage media on that device.

15.2 Use of work phones by staff
Some members of staff are provided with a mobile phone by the school for work purposes, e.g. staff working in Laughalots and lead teachers on school trips. Only authorised staff are permitted to use school phones for work purposes and conduct linked to the device will be professional at all times.

15.3 Use of mobile phones and other personal devices by pupils
Pupils are prohibited from using mobile phones, smartwatches, cameras or any other recording equipment at school.

Pupils must not take, use or share photographs, video or audio recordings on school premises unless specifically authorised by a member of staff. Any school use of images or recordings will follow the school's data protection, safeguarding and image-use procedures. Whether data protection law applies, and the appropriate lawful basis, will depend on the circumstances; lack of consent does not by itself establish that legislation has been breached.

Some pupils in Year 5 and Year 6 walk to and from school unaccompanied but written consent from parents/carers is required. These pupils have permission to bring a mobile phone into school, should their parents wish them to.

Save for exceptional circumstances authorised by the Headteacher, the mobile phones **must** be switched off on arrival at the school gate and handed to the class teacher on arrival at the classroom. Devices will be stored in a safe place for the duration of the school day.

The class teacher will return devices to the children at the end of the school day but phones must be placed straight into school bags as they must not be turned on until a pupil has left the school premises.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport to and from school, during school visits or trips, or while pupils are travelling to or from school.

Pupils will be taught the risks that are associated with the use of mobile phones as part of our PDL and online safety curriculum (see Section 9).

Exceptional circumstances
When there is a medical or SEND need for a device (e.g. for a diabetic child), then phones are permitted but these devices must be locked down for all purposes other than the medical apps.

15.4 Sanctions
- Staff that fail to adhere to this policy may face disciplinary in line with the school's Disciplinary Policy.
- Where authorised staff confiscate a device as a disciplinary penalty, confiscation will be lawful, reasonable and proportionate, recorded, and carried out in accordance with the behaviour policy and DfE searching, screening and confiscation guidance. The school will decide promptly when and to whom the device will be returned, normally the pupil or parent/carer, having regard to safeguarding, evidence preservation and the circumstances of the incident. Any examination or deletion of data will occur only where the statutory power and published school policy permit it. Parents will be informed if their child has been in breach of this policy and will be advised of the sanction. In each case, the sanction given must be reasonable and proportionate.

15.5 Safeguarding
A pupil's behaviour with a personal device may indicate they may be suffering, or at risk of, harm. If this is suspected, staff will follow the appropriate procedure set out in Keeping Children Safe in Education. This will include speaking with the Designated Safeguarding Lead (DSL) or Deputies, who will consider whether pastoral support, an early intervention, or a referral to children's social care is appropriate.
Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously and will involve the police or other agencies as appropriate.

15.6 Use of personal devices by parents/carers, volunteers and visitors
Parents and carers are encouraged to reinforce and discuss this policy at home as appropriate, including the risks associated with mobile phone use and the benefits of a mobile phone-free environment.
Parents and carers are encouraged to refrain from using their mobile phones on school site in the presence of pupils. There may be some exceptions, such as:
- In celebration assemblies or pupil performances, parents may be invited to take photos of their child but the school will remind parents that they must not post photos of other children on social media for safeguarding reasons.
- A volunteer on a school trip may be invited to check their device during a break and will be encouraged to do this away from pupils.

School trips: Volunteers supervising school trips or residential visits must not use their phone to make contact with other parents/carers. Additionally, they must not take photos or recordings of pupils, their work or anything that could identify a pupil.
Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

16. Social media

The School intends to use social media as a method of connecting and collaborating with our school community in a way that reflects 21st Century communication. We require that all interactions with school social media networks reflect our school vision *'Children at our heart, Christ at our centre, We love, we learn and we live'.* Overall, we are working together to achieve a positive, informed, communicative school community.

16.1 Official school social media
The school's official social media channels are:
- The School website: www.saintanthonysfareham.co.uk
- Facebook (AnthonyFareham)

These accounts are managed by office staff and the Headteacher.
The school will post: alerts, reminders, advertisements, achievements, photos, seasonal greetings.
The school will not post: names and photos without consent, harmful comments, political statements.

16.2 Code of Conduct
Users must use real names (so that school can identify the user).
Posts must use first names and not raise individual issues publicly (see Section 8)

16.3 Administration
The Leadership team will monitor social media in line with this policy, parents' consent to the 'Home school agreement' and the staff Code of Conduct.

17. Response 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. 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/staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

18. Training

The governing board, through the Headteacher, Will ensure that every member of staff, including staff who do not work directly with children, read Part One of Keeping Children Safe in Education 2026 in full, receives appropriate safeguarding and child protection updates at least annually and more frequently as required, and understands the school's filtering and monitoring arrangements and their individual responsibilities.

The DSL and Deputy DSLs undertake child protection training including online safety at least every 2 years, with annual updates.

19. Related policies

This Safe Use of Technology policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy
- Complaints procedure
- Business Continuity Plan

Appendix 1: Acceptable use agreement for pupils

St Anthony's is committed to safeguarding and promoting the welfare of children. All pupils use computer facilities including online access as an essential part of learning, as required by the national curriculum.

Key Stage 1 guidance (Year 1 & 2):

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.





We can send and open emails together.

We can write polite and friendly messages or emails to people that we know.



Lower Key Stage 2 guidance (Years 3 & 4):

Think then Click

e-Safety Rules for Key Stage 2



- We ask permission before using the Internet.
- We only use apps or websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send messages, e-mails and attachments that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not share passwords with other people
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.



Upper Key Stage 2 guidance (Years 5 & 6):

Think then Click

e-Safety Rules for Key Stage 2



- We ask permission before using the Internet.
- We only use apps or websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send messages, e-mails and attachments that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not share passwords with other people
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We do not bring our phones to school – if we need a phone because we walk home, we will give it to our class teacher who will look after it during the day.



Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the Internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL or Deputies) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Acceptable use agreement for parents and carers

This agreement is usually incorporated to an online 'home school agreement' that parents are asked to sign at the start of each academic year.

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Tapestry • Email/text groups for parents (for school announcements and information) • Occasionally (for general updates) our Facebook page Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 4: 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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you use a unique, sufficiently long password or approved passkey for school systems, enable multi factor authentication where available, and change credentials promptly if compromise is suspected or required by the school?	
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 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 6: The ethical framework for AI in education

European Commission:

Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for Educators

UNESCO:

