St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

St Mary's Church of England Primary School

ICT, Personal Device and Internet Acceptable Use Policy

Adopted: 6th January 2024 Review date: Spring 2025

Contents

1. Introduction and aims 2
2. Online safety 3
3. Definitions 3
4. Unacceptable use 3
5. Staff (including governors, volunteers, and contractors) 4
6. Pupils 8
7. Parents 9
8. Data security 9
9. Internet access 10
10. Monitoring and review 11
11. Related policies 13
Appendix 1: Facebook cheat sheet for staff 14
Appendix 2: Acceptable use of the internet: agreement for parents and carers 16
Appendix 3: Acceptable use agreement for older pupils 17
Appendix 4: Acceptable use agreement for younger pupils 18
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors 19
Appendix 6: Guidance on data protection 18

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors;
- Establish clear expectations for the way all members of the school community engage with each other online;
- Support the school's policy on data protection, online safety and safeguarding;
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems;
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Behaviour Policy (pupils) or Disciplinary Procedure (staff members).

School Vision

The school's ICT, Personal Device and Internet Acceptable Use Policy reflects our Christian vision:

"Love one another. As I have loved you, so you must love one another." John 13:34

Unconditional love underpins all we do at St Mary's Church of England Primary School. We value and embrace the individuality of every child as they discover, learn and flourish in a place of security and love. We are an inclusive school, welcoming all children with respect, understanding and dignity. We have a duty of

care to the children and will demonstrate the compassion and understanding that allows all children to flourish. In the context of the ICT, Personal Device and Internet Acceptable Use Policy, the primary message of the school's vision is that we must protect children from harm and treat all members of the school community with the dignity and respect that will allow them to flourish.

2. Online Safety and Filtering and Monitoring

Acceptable use of ICT, personal devices and the internet relates closely to the school's policies and procedures with regard to safeguarding. The following information about online safety is taken from section 10 of the school's Child Protection and Safeguarding Policy.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation and technology often provides the platform that facilitates such harm.

The Local Governing Body has had due regard to the additional information and support set out in KCSiE and ensures that the school has a whole school approach to online safety, and has a clear policy on use of communications technology in school. Online safety will be a running and interrelated theme when devising and implementing policies and procedures. This will include considering how online safety is reflected in all relevant policies and whilst planning the curriculum, any teacher training, the role of the DSL and any parental engagement.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school adopts a whole school approach to online safety to protect and educate pupils and staff in their use of technology, and establishes mechanisms to identify, intervene in, and escalate any concerns as appropriate.

Online safety issues can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, or radicalisation or extremism;
- **Contact**: being exposed to harmful online interaction with other users, for example, peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct**: online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and online bullying); and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If staff feel that either they or pupils are at risk this should be reported to the Anti-Phishing Working Group (https://apwg.org/).

The governing body will ensure that an annual review is undertaken of the school's approach to online safety including the school's filtering and monitoring provision, supported by an annual risk assessment that considers and reflects the risks pupils face online. The review should include a member of the senior leadership team, the DSL, the IT service provider and a governor. The school should ensure they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on cyber security including considerations can be found at Cyber security training for school staff - NCSC.GOV.UK

The school uses Smoothwall Monitor filtering and monitoring software, managed by the school's IT Technician in conjunction with the Online Safety Lead.

The school's online safety policy outlines the appropriate filtering and monitoring which take places on school devices and school networks. It also outlines the expectations, applicable roles and responsibilities in relation filtering and monitoring.

School staff can access resources, information and support as set out in Annex B of KCSiE.

The Acceptable Use of ICT, Personal Devices and Internet Policy reflects the fact that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school can sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. The school considers carefully how this is

managed on the premises and reflects this in the Acceptable Use Policy and Online Safety Policy. The school ensures that children do not have use of, or access to, mobile phones whilst on school premises. The school arranges to look after pupils' mobile phones during the day – these are handed in at registration.

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs
- **"Personal Device":** any device that is internet-enabled via Wi-Fi or mobile networks, such as mobile phones, tablets or wearable technology, including smart watches

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or 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
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher (or Deputy Headteacher / Senior Teacher in the Headteacher's absence) will use 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

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

The Headteacher will discuss any exceptions with the Chair of Governors, who will report on this in the next Local Governing Body meeting.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's Behaviour Policy and Disciplinary Procedure.

The Headteacher (or Deputy Headteacher / Senior Teacher in the Headteacher's absence) will make a professional judgement about whether a person's permission to access the school's ICT systems, network or broadband internet should be restricted or revoked. This is the Headteacher's discretion. Such sanctions will be discussed with the Chair of Governors, who will report on this in the next Local Governing Body meeting.

The school's Behaviour Policy can be found on the school's website. The Code of Conduct and Disciplinary Procedure can be found on the staff 'shared drive' or can be requested from the school office.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's IT Technician (Luke Frost IT Services) manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Technician.

5.1.1 Use of phones and email

Email is a vital business tool but must be used with great care and discipline. Staff should always consider if email is the appropriate method for a particular communication. Correspondence with third parties by email should be written professionally. Messages should be concise and directed only to relevant individuals.

The school provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided. Personal email accounts must not be used for work emails. Email between School or MAT accounts is secure. Email from School or MAT accounts to an external account is not. Given this, if confidential information or personal data is to be emailed to a non-School or MAT account, the confidential information/personal data must be included within a password protected document (with a strong password, which is different every time) and the password must be provided to the recipient by a non-electronic means

(e.g. by telephone call). Where encrypted email systems are in operation, it is acceptable to transmit confidential information without further security.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform an administrator or Senior Leader immediately, who will refer the issue to our Data Protection Officer (data.protection@schoolschoice.org) and follow our data breach procedure.

Staff should ensure that they access their emails at regular intervals throughout each working day and stay in touch by remote access when travelling. If staff are aware that they will be unable to access their email for a prolonged period (e.g. in the case of a planned medical procedure) they must agree with the Headteacher whether their email will be forwarded onto a colleague.

Staff must endeavour to respond to emails marked "high priority" within 24 hours (in relation to working days). Staff must not label emails as “high priority” inappropriately.

Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone doing this will face disciplinary action. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via email, should inform the Headteacher.

Staff must take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff must assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Email messages may be disclosed in legal proceedings in the same way as paper documents or as part of a subject access request under the general data protection regulation (GDPR). Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. **All email messages should be treated as potentially retrievable, either from the main server or using specialist software.**

Staff must not: (a) send or forward private emails at work which they would not want a third party to read; (b) send or forward chain mail, junk mail, cartoons, jokes or gossip; (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them; (d) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter; (e) download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this; (f) send messages from another member of staff's computer or under an assumed name unless specifically authorised

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Users should take note of the following guidance from the school’s Code of Conduct:

As with all personal possessions, the school is not responsible for the security of personal devices. Staff members must be sensitive about their roles in school and personal devices, including mobile phones, should only be used at appropriate times.

- Phones should be silent during lesson times.

- Employees should not make or receive calls in front of pupils or during lesson times or during times when they are expected to be working (i.e. not break times).
- Phones should not be used to record and keep images or footage of pupils.

It is recognised that imposing rigid regulations or 'bans' can be counterproductive and can lead to a culture of secrecy, suspicion and uncertainty. Therefore, this code operates on a basis of professional trust with regard to the use of personal mobile phones. There may be times when exceptional personal circumstances require more flexibility. This should be negotiated with a Senior Leader or the Headteacher.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or may restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with pupils, parents or professional colleagues, e.g. during lessons or training sessions;
- Does not constitute 'unacceptable use', as defined in section 4;
- Takes place when no pupils are present;
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes;
- Does not impact on work efficiency or costs;
- The level of use is reasonable (as determined by the Headteacher) and not detrimental to the main purpose for which the facilities are provided;
- Is not of a commercial or profit-making nature;
- Is not of a nature that competes with the business interests of the school or conflicts with an employee's obligations.

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones, smart watches or tablets) in line with the school's Code of Conduct and provided that personal devices are not used for unacceptable purposes as defined in section 4. Personal devices should only be used according to the principles outlined above in relation to the school's ICT facilities.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

Only the IT Technician is able to access the school's IT systems remotely. School staff members with the appropriate level of access are able to access cloud-based systems, such as Target Tracker, CPOMS, BromCom and the Welfare Call EPEP system.

We allow users to access the school's ICT facilities and materials and cloud-based systems remotely for authorised business use only. Only those users who would ordinarily have relevant permissions and access internally are able to access systems remotely.

Users accessing the school's ICT facilities and materials and cloud-based systems remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the IT Technician or Headteacher may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the St Edmundsbury and Ipswich Diocesan Multi Academy Trust Data Protection Policy (available on the MAT website or on request from the school office) and the guidance in Appendix 6 (taken from Appendix 3 of the Code of Conduct).

5.4 School social media accounts

The school has an official Facebook page, managed by designated staff member or a school administrator. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The guidelines below set out what can and cannot be posted on the school's social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool requires the approval of the Headteacher. Users must not set up social media sites or channels seeking to represent the school without this approval. The Headteacher may restrict or stop the use of official social media sites at any time at their discretion.
- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Staff use school-provided email addresses to register for and manage any official social media channels.
- Official social media sites are suitably protected and linked to our website.
- Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with relevant school policies and must not be used for unacceptable purposes as defined in section 4 of this policy.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Written parental consent will be obtained, as required, for use of pupils' data (such as photographs) in social media communications and posts.
- All social media communications and posts must be respectful of all members of the school community and should not be used to make complaints. Any complaints must be made according to the formal procedures for this.
- Staff members should not enter into ongoing dialogue with other social media users. Social media communications are only to be used for posting official school news or information.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

- Computers and the school's ICT equipment are available to pupils only under the supervision of staff.
- Pupils should not seek to use school ICT equipment without permission or for purposes other than those set out by staff members. If they do so, they would be subject to the school's Behaviour Policy.
- Pupils' personal internet-enabled devices, such as mobile phones and smart watches must be handed in at the school office, where they are kept in the safe. Pupils are not allowed access to personal devices in the classroom, the toilets / changing rooms or other areas within the school.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or 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

- 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
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. Pupils are taught about security as part of the approach to teaching online safety.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Headteacher. For the avoidance of doubt, on the termination of employment (for any reason) staff system accounts are suspended and staff are required to return any equipment, keys or security fobs. The Headteacher is responsible for notifying the HR team when staff are known to be leaving and the HR team will then liaise with IT support to ensure that appropriate controls are put in place and that accounts and access are cancelled/redirected as soon as the member of staff has left.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Staff must not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the School or exposing it to risk. Unencrypted USB memory sticks – or similar – must not be used to transfer any school data (which includes resources and materials produced by staff) to or from school, or between devices (regardless of whether these are owned by the school or personal devices). Staff must not download or install software from external sources without receiving authorisation from the Headteacher. Incoming files and data must always be virus-checked before they are downloaded (this will generally be done automatically but, if in any doubt, staff must seek advice from IT support). No device or equipment should be attached to our systems without authorisation from the Headteacher. For the avoidance of doubt, this includes any USB flash drive, MP3 or similar device, PDA or smartphone. It also includes use of the USB port, infrared connection port or any other port although it is acceptable to plug personal devices into the School's systems, solely for the purpose of charging. It is acceptable to attempt to join School's WiFi networks without prior authorisation, where guest arrangements exist.

Staff using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use when off site and take any precautions required by IT support from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the St Edmundsbury & Ipswich Diocesan Multi Academy Trust's Data Protection Policy. Any data breaches must be reported to administrative staff or the Headteacher, who will in turn report to the Data Protection Officer (Schools' Choice Data Protection Service data.protection@schoolschoice.org). Guidelines related to data protection can be found in Appendix 6.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by IT Technician.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert IT Technician immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff must only use devices (including computers, tablets and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school. Personal devices should not be used for these purposes or conducting any school business. In exceptional circumstances, the Headteacher may authorise this temporarily but permission should not be assumed and should not be a permanent arrangement.

9. Internet access

The school wireless internet connection is secured.

- The school's broadband internet provider is Excell. Excell use a Fortinet Firewall system for filtering on the school's behalf. On occasions when the firewall fails to filter out inappropriate content, staff members must notify a senior leader, the Computing Leader or administrator as soon as possible. They will notify the IT Technician who will contact Excell on behalf of the school to request that the website be blocked. Pupils are taught what to do if inappropriate websites are accessed by accident (in all circumstances, they should report to an adult in the classroom immediately). Appropriate sites that have been filtered in error are reported in the same way.
- Parents are not given access to the school's Wi-Fi codes. The school has an internal Wi-Fi network and a separate Wi-Fi system that can be used for guests to provide additional security.
    - **St Mary's Internal** - This is to be used by all school bought devices (laptops, iPads, desktops, printers etc.)
    - **St Mary's Wi-Fi** - This is to be used by everything else (mobile phones, external providers that come in etc.)

9.1 Pupils

Pupils use the school's network and Wi-Fi systems for educational purposes only. Wi-Fi is available throughout the school to support learning. Pupils are taught about the importance of security and suitable passwords as part of online safety teaching. Staff members provide pupils with passwords for them to use to access ICT systems and specific programs used in school. Pupils are not allowed to access the school's network or Wi-Fi using personal devices and the Behaviour Policy will be applied if they attempt to do so. All pupils who access the school's network have their own log-in details and are strongly discouraged from sharing these.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher (or Deputy Headteacher / Senior Leader in the absence of the Headteacher). Visitors requiring access to the school's Wi-Fi are only allowed to access the 'guest' Wi-Fi ('St Mary's Wi-Fi').

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity, e.g. as a volunteer, although it is extremely unlikely that access would be granted for personal devices and there would need to be a clear benefit to the school;
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access training materials stored on personal devices as part of a presentation or lesson plan).

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action. Parents or other visitors authorised to access the school's Wi-Fi are given passwords on the condition that these will not be shared.

Photographs of pupils must not be placed on personal social networking sites or the school's website without parental or guardian consent. This is personal related data and individuals must be aware that this information is being published. Failure to obtain consent could result in formal action being taken. Parents and visitors must not use personal devices within school to take photographs of other people's children.

10. Digital and Video Images

In accordance with guidance from the Information Commissioner's Office (ICO), parents/carers are welcome to take videos and digital images of their children at school events (including school organised activities out of school) on their personal equipment for their own personal use. To respect everyone's privacy, members of staff should make parents/carers aware that these images (in particular images including children who are not their own) must not be published/made publicly available whether on social networking sites or otherwise.

Teaching and support staff are allowed to take digital/video images to support educational aims. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the school into disrepute.

Photographs/video published on the school's websites, or elsewhere, which include pupils will be selected carefully and permission will be sought from the relevant parent/carer. The names of pupils who appear on images/video will not be published, other than with the prior, explicit consent of the parent/carer.

Video conferencing is a tool which the school may use to support learning, for example during a period of school closure. Permission for this will be sought from parents/carers prior to this taking place. The school may make recordings of video conferences to support educational aims. Where a video conference involves participants from outside of the MAT, permission must be requested in advance of making a recording. Video conferencing is always supervised by a competent adult, who knows how to end the call if necessary. The adult who supervises the call is responsible for switching off the camera at the end of the call.

11. Monitoring and review

The Headteacher, Senior Leaders, the IT Technician and the Computing Leader monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed and approved by the Local Governing Body every two years.

12. Related policies

This policy should be read in conjunction with other significant documents, policies (produced by the school and the St Edmundsbury & Ipswich Diocesan Multi Academy Trust) and procedures, including:

- Teachers' Standards
- Child Protection and Safeguarding Policy;
- Anti-Radicalisation Policy;
- Whistleblowing Policy;
- Safer Recruitment Policy;
- Staff Handbook;
- Online Safety;
- Code of Conduct;
- Data Protection Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Disciplinary Procedure.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

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: • Our official Facebook page • Email/text groups for parents (for school announcements and information) 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 if they aren't 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 other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: 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 private businesses, 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) 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 6: Data Protection (taken from the Code of Conduct)

At St Mary's C of E Primary School, policies and procedures are designed with privacy and security at their core.

Staff members are expected gather, store, process and, if necessary, share personal data with great care. Personal data refers to any electronic or hard copy information relating to a person (data subject) that can be used directly or indirectly to identify the person.

All staff members must be aware of the following rules and guidance within school that relate to how personal data should be gathered, stored, processed or shared. Sensitive use of personal data is considered to be a key aspect of good professional conduct.

- Staff members **must** only use memory sticks that are encrypted and supplied by the school.
- Staff members are **advised** to always keep memory sticks in the same place to avoid them getting lost.
- Staff members **must** only use password-protected laptops supplied by the school for school work off-site.
- Staff members **must** not leave school laptops in cars overnight.
- School email **must** only be used for work purposes. Emails containing sensitive information **must not** include pupils' full names. Sensitive documents sent via email to external agencies **must** be password protected (passwords should be sent in separate emails).
- Personal data taken on school trips for safety reasons **must** be shredded on return to school.
- Staff members are **advised** to use the shredding service paid for by the school to dispose of confidential documents. Documents for shredding should be put into the shredding bags in the lockable walk-in cupboard in the school office.
- Confidential documents **must** not be left on the central printer in the entrance hall after printing. In order to avoid this, staff members should not print off documents sent to the printer by another user.
- The main office **must** always be locked when unattended. The Headteacher's office **must** be locked overnight.
- Staff members are **advised** to limit the amount of personal data taken off-site for meetings or working at home, taking only the documents that are relevant and necessary to contribute professionally to the meeting or undertake the work.
- There **must** be a professional, justifiable reason for taking pupils' blue files or safeguarding files off-site. If blue files or safeguarding files are taken off site, they **must** be signed out and back in on return. The sheet for signing out these files is kept in the main office.