ICT & Internet Acceptable Use Policy

Date	Review Date	Coordinator	Nominated Governor
December 2022	December 2023	M. Pavey	A. Lambert

Introduction and aims

St. Michael's is a happy school where the pupils and staff share many magic moments together. It is filled with imagination, nurture, enthusiasm, creativity, risk-taking and challenge. As a Church school, our Christian ethos weaves its way throughout all that we do to make our school the special place it is.

Information and Communications Technology (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 Staff Code of Conduct 2022 and Child Protection and Whistle Blowing policies.

Relevant legislation and guidance

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

Data Protection Act 2018
The General Data Protection Regulation
Computer Misuse Act 1990
Human Rights Act 1998
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Education Act 2011
Freedom of Information Act 2000
The Education and Inspections Act 2006
Keeping Children Safe in Education 2022
Searching, screening and confiscation: advice for schools

LOTTERY FUNDED

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

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 Sanctions 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

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher, Deputy Headteacher, Computing Subject Leader and relevant governors 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.

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 user will require written permission from the Headteacher in order to carry out their given purpose.

Sanctions
Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Behaviour Policy, Online Safety Policy and Staff Code of Conduct.

Sanctions for any of the unacceptable activity listed above are circumstantial and depend on the user in question. It may include:

- Removing the right to access technology provided by the school.
- Informing any relevant external authorities such as the police.
- Where children have misused technology, their parents will be informed.

Copies of the above policies which dictate disciplinary action can be found on the school website at https://www.stmichaelsaldbourne.co.uk/our-school/school-policies/.

Staff (including governors, volunteers, and contractors)
Access to school ICT facilities and materials
The school's network manager, Oakford Technology, 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 Oakford Technology. Where appropriate, permissions may also be required from the senior leadership team.

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.

All work-related business should be conducted using the email address the school has provided.

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 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.

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

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 Oakford Technology and the Headteacher immediately and follow our data breach procedure.

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.

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. Oakford Technology, the Headteacher or the Computing Subject Leader may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with children
- 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
- Takes place on the school premises.

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. 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 or tablets) in line with the school's Acceptable Use Agreement.

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.

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

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

Staff use of personal devices
Allowing the use of mobile devices is a school decision, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use
- Users connect their device to the school's wifi so that their device is subject to the school's filtering policy. This includes visitors to the school, such as peripatetic teachers.

St Michael's School policies regarding the appropriate use and sharing information apply to devices both school and privately owned. Use of any device must adhere to data protection, online safety and health and safety rules. A device connecting to the school network may be configured with certain restriction in place. Any settings that are passcode protected must not be changed.

Staff should keep their personal phone numbers private and not use their own mobile phones to contact children, young people or parents. They should never share their log-ins or passwords with other people.

Staff should not give their personal e-mail addresses to children, young people or parents. Where there is a need for correspondence or written information to be sent electronically the work e-mail address should be used.

Personal devices should not be used in the presence of children. During the school day, personal devices should be kept in a secure place out of sight of children.

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 Social Media Policy).

Remote access
We allow staff to access the school's ICT facilities and materials remotely.

Oakford Technology provide software that enables staff to access the necessary materials outside of the workplace. Security arrangements include the use of a username and password. Remote access is installed onto staff laptops but in instances where the software cannot be found, a request can be submitted to Oakford Technology for this to be set up by staff.

Staff accessing the school's ICT facilities and materials 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 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 our data protection policy.

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

The school's data protection policy can be found online at https://www.stmichaelsaldbourne.co.uk/our-school/school-policies/.

School social media accounts

The school runs the following social media accounts:

- Forest School Facebook
- Continuous Provision Facebook
- Whole school Facebook
- Continuous Provision Instagram
- Vimeo
- School blog
- Weduc

These are managed by the Headteacher, Deputy Headteacher and several members of the teaching staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account. All members of the St Michael's community will be encouraged to engage in social media in a positive, safe and responsible manner at all times. Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community (staff, children, parents, governors or volunteers).

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times. The guidelines can be found in the school's Social Media Policy.

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
- Ensure that use of social media complies with the social media policy

Pupils

Access to ICT facilities

Students have access to a set of laptops and iPads. They are to be used under direction from teachers and strictly for educational purposes, which include, but are not limited to:

- Research relating to the wider National Curriculum conducted through the internet.
- The Computing curriculum

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

- Interventions
- Apps designed for use in other areas of the curriculum, including but not limited to Times Table Rockstars (TTRS), Nessy Reading & Spelling and BBC Dancemat

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.

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
- Sanctions will be set in line with the school's behaviour policy.

Parents
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 or as a member of the PTA) 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.

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.

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

We ask parents to sign the Acceptable Use Agreement for Parents/Carers.

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.

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.

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.

Data protection
All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

The school's data protection policy can be obtained from the school office upon request.

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 Oakford Technology.

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 either the Headteacher, Deputy Headteacher, Computing subject leader or Oakford Technology 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 and closed down completely at the end of each working day.

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

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by Oakford Technology.

Internet access
The school wireless internet connection is secured. The school uses a filtering system to prevent access to inappropriate websites. However, the school recognises that filters aren't fool-proof and that there will be instances when an inappropriate website will not be identified. There will also be instances where an appropriate website has been filtered in error. All such cases should be reported to Oakford Technology who can address the issue accordingly. The school does not typically provide access to the school's wireless internet connections for parents and the public except in certain circumstances agreed by Headteacher and other senior leaders. There are also two separate connections for devices used by either staff or pupils.

Pupils
Devices such as laptops or iPads that are used by pupils automatically connect to the internet. The filtering systems as explained above are applied to all devices while connected to the internet in school. Where a device has, for any reason, not connected to the internet, the pupil should ask their teacher to help reconnect their device to the internet. Any continuing connectivity issues should thereafter be reported to Oakford Computing.

Parents and visitors
Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review
The Headteacher, computing subject leader and Oakford Technology 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 every two years.

The governing board is responsible for approving this policy.

Related policies
This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff code of conduct
- Data protection

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED

Appendix 1: 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 understand the behaviours and expectations required of me when running official school social media channels to ensure that these sites are used safely, responsibly and in accordance with local and national guidance and legislation. I will connect all personal devices to the school's wifi so that their device is subject to the school's filtering policy. 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:**

St Michael's CofE (Aided) School
Back Lane, Aldbourne, Wiltshire SN8 2BP
01672 540434 - admin@stmichaelsaldbourne.co.uk

LOTTERY FUNDED