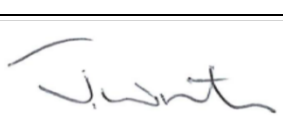
ICT Policy

Thomas Keble School

Signed by The Chair of Trustees Mr Julian Wintle:	
Implemented:	08 May 2025
Review date:	08 May 2028
Author:	S Allan

Contents

1. AIMS:

1. To establish safe and secure ICT systems and procedures, keeping abreast of developments in communication and information management to maximise the benefits for all members of the school community while minimising the risks for all users.
2. To promote responsible and appropriate use of ICT by all members of the school community.
3. To establish effective and secure data management procedures.
4. To promote best practice in the acquisition, ongoing management and disposal of ICT equipment, including the consideration of environmental issues.
5. Support the school in teaching pupils safe and effective internet and ICT use

2. OBJECTIVES:

1. To educate all pupils in the safe and appropriate use of the school's ICT systems, and put systems in place that supports their safety in this regard.
2. To enable all pupils in the school access to appropriate ICT resources to effectively support their learning.
3. To ensure that all staff can access ICT resources to support their work within the school.
4. To ensure compliance with the Data Protection Act.
5. To ensure that all staff, governors and other appropriate individuals are fully aware of safe procedures with regard to data they may have access to in the course of their work.
6. To clarify expectations of pupil behaviour when using ICT equipment.
7. To clarify appropriate staff use of the school's ICT equipment.
8. To ensure that systems are in place to monitor the use of ICT in school.

3. USE OF ICT EQUIPMENT – PUPILS:

All pupils are provided with a password protected user account for their IT based work, along with a school email address. Pupils should be able to 'log-on' to the network and access these facilities when required to do so for work in a lesson or other appropriate time. All pupils must ensure that they follow guidelines for responsible use indicated in their planner, displayed in the ICT rooms, and referred to in the Home-School Agreement. Pupils must not act in a way that is clearly at odds with the notion of responsible use. Examples of such behaviour would include:

- Sharing passwords with others, or accessing the user account of any other pupil.

- Downloading, or attempting to download, anything from the internet which is not for the purpose of supporting their work in school.
- Accessing, or attempting to access, websites or files that contain inappropriate material.
- Using school ICT equipment to access internet chat rooms or 'social networking' sites.
- Attempting to bypass the school's systems for ICT security and filtering by, for example, the use of proxy websites.
- Any attempt to interfere with or disrupt the operation of the school's ICT resources.

In addition to the use of the network within curriculum time, pupils can access their resources at lunchtimes and after school in the library. Additional expectations for the use of the network at these times are published by the library and reviewed on a regular basis.

Pupils who misuse ICT equipment in lessons must be dealt with by the teacher concerned in line with the school's Behaviour Policy, with a report of the incident also being forwarded to SMT and IT Support Manager as appropriate.

4. STORAGE AND USE OF DATA – PUPILS

Pupils will only be granted access to their own area of the network and the "Pupil Shared" and Resources areas. Pupils must not, under any circumstances, be granted access to the data in the drives reserved for staff use or to the school's information management software (SIMS). The school regularly backs up the data stored by pupils on their network area, as described in the 'Security' section below.

5. STORAGE AND USE OF DATA – STAFF

Staff have access to their own storage area, the Pupil Shared, Resources and Staff Share areas, and a Shared Admin area if appropriate to their role. Staff also have access to data on individuals via the school's information management software (SIMS) – this data is covered by the Data Protection Act. Staff must ensure that they access and use this data safely and responsibly. Staff must not make their own copy of this data on, for example, laptop hard-drives, USB devices, compact discs or any other storage media, including forwarding data to their own private email accounts. If such data is printed out it must be kept securely until needed and then disposed of appropriately.

With regard to the work that pupils carry out and store on the network, staff should be aware that when the work includes the names, addresses or other personal information of any individuals, the data protection act may then apply to that piece of work. Such work should be stored on the network for no longer than necessary.

Governors have access to information and papers regarding the business of the school. Where access to such papers is via electronic communication, Governors should be mindful of any potentially sensitive issues and ensure that appropriate storage and printing arrangements are adhered to.

Platforms, apps or devices **not** authorised by the school for work use (e.g. personal email accounts, personal mobile phones) must not be used to share pupils' or staff personal data or information about confidential or sensitive school business. The authorised electronic communication methods are school email, Egress secure email, SIMS, and school mobile phones.

6. USE OF ICT EQUIPMENT – STAFF

All staff are provided with a password protected user account on the school's network, along with a school email address. Staff must take every reasonable measure to protect their password, change it at regular intervals, and immediately inform the IT Support team if there is any suspicion that the security of the network has been compromised.

All full-time teaching staff, and a number of other staff, are provided with a laptop to support their work – when such equipment is issued to staff, it is expected that the predominant use of the equipment will be to support teaching and learning in the school and that the equipment will be present in school during the school day. The IT Support team will, from time to time, need to take back such equipment for checking and upgrading. Similarly, the IT Support Manager may issue guidance for staff on the efficient use of their equipment (for example, with regard to the storage and back-up of files) and staff must take full account of such guidance. Staff must take all reasonable steps to ensure the safety and security of any equipment issued to them by the school.

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 must take such precautions as the operations manager or headteacher may require against importing viruses or compromising system security.

7. INTERNET SAFETY

The approach adopted to maximise the safety of pupils when using the internet includes education with regard to possible risks and how to minimise them, as well as monitoring and control systems, such as filters, that are put in place and developed by the IT Support Manager.

The school works with appropriate agencies (such as the police and SWGfL) to provide accessible, reliable and up-to-date information for pupils to ensure that they are as safe as possible in their use of the internet and other means of electronic communication. The topic of Internet Safety is included as appropriate in Computing lessons and tutor work. The content of the work is regularly reviewed by the school's e-safety committee (see 'Security' below).

The school's internet access is provided by BTNet. The service includes the provision of an appropriate firewall. The filtering system and monitoring is provided by an internal system Smoothwall. The school actively blocks inappropriate websites as required and has installed additional hardware and software to monitor the websites visited by all users of the network.

8. MONITORING

All users of the school's network and other ICT facilities may have their activities monitored for the purposes of the safety and security of the network, and to ensure that the expectations for appropriate use are adhered to. If the monitoring process indicates inappropriate activity by any individual, the matter will be reported to the SMT member with responsibility for ICT and/or directly to the Headteacher.

9. SECURITY

The school will take all possible steps to ensure the security of ICT equipment, including the maintenance of an accurate and up-to-date inventory. All ICT equipment is marked with Selecta DNA as a deterrent to theft.

The school's servers are backed up on a daily basis, via a secure and encrypted on-line service which allows information to be restored (max. 3 months).

10. SUSTAINABILITY

Computer purchases are made in accordance with the principles of best value as well as considerations of energy use. All staff must ensure that they adhere to the guidelines provided for shutting down computers when appropriate.

The school will always ensure that ICT equipment is disposed of by the most appropriate method, making use of schemes that refurbish and re-use the equipment in other settings whenever possible. If this is not a viable option, recycling schemes that re-use individual components and dispose of waste appropriately will be used.

11. UNACCEPTABLE USE

Unacceptable use of the school's ICT facilities includes are referenced in the Staff Code of Conduct, Section 17, pages 26 to 28. In addition:

- 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

12. USE OF PHONE AND EMAIL

- The school provides each member of staff with an email address.
- 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/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.
- 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 that contains the personal information of another person, they must inform the IT helpdesk and the Headteacher immediately and follow our data breach procedure.
- Staff must not give their personal phone number(s) to parents/carers 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.

13. RECOMMENDATIONS REGARDING SOCIAL MEDIA

Please refer to the Staff Code of Conduct, Section 8, pages 13 to 15. In addition:

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
- Check your privacy settings regularly
- Be careful about tagging other staff members in images or posts
- Don't share anything publicly that you wouldn't be happy showing your pupils
- Don't use social media sites during school hours
- Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
- 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)
- 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
- 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 students or parents).