Policy Owner	Cindy Burstin
Approving Body	Board of Governors
Date Approved	February 2023
Effective Date	February 2023
Review date	February 2026

Staff IT Acceptable Use Policy

St. Aubyn's School

1 **Introduction**: This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT in connection with your job including:

1.1 the School's email and internet services;

1.2 telephones;

1.3 the use of mobile technology on School premises or otherwise in the course of your employment (including 3G/4G/5G or Bluetooth or other wireless technologies), whether using a school or a personal device; and

1.4 any hardware (such as laptops, iPads, printers or mobile phones) or software provided by, or made available by, the School.

This policy also applies to your use of IT off school premises if the use involves Personal Data of any member of the School community or where the culture or reputation of the School are put at risk.

2 **Failure to comply**: Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

3 **Property**: You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Bursar and IT Department. You should not use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4 **Viruses and other malicious code**: You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the IT department.

5 **Passwords**: Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number and/or character. Your password should not be disclosed to anyone else. In addition:

5.1 your password should be difficult to guess, for example, you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday;

5.2 you must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account;

5.3 passwords (and any other security credential you are issued with such as a key fob, alarm fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

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

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

6 **Leaving workstations**: If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access.

7 **Concerns**: You have a duty to report any concerns about the use of IT at the School to the Deputy Head or the Bursar. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Other policies**: This policy should be read alongside the following:

8.1 Staff Code of Conduct;

8.2 Data Protection Policy for Staff;

8.3 Acceptable Use Policy for Pupils;

8.4 Online Safety Policy;

8.5 Remote Learning Policy

8.6 Staff Social Media Policy

8.7 Staff Communications Policy

Internet

9 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited

10 **Personal use**: The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for unacceptable purposes (as described in section 17 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Head.

11. **Unsuitable material**: Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or mobile data when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

12 **Location services**: The use of location services represents a risk to the personal safety of those within the School community, the School's security and its reputation. The use of any website or application, whether on a School or personal device, with the capability of publicly identifying the user's location while on School premises or otherwise in the course of employment is strictly prohibited at all times.

13 **Contracts**: You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from the Bursar. This applies both to "free" and paid for contracts, subscriptions and Apps.

14 **Retention periods**: the School keeps a record of staff browsing histories for a period of 3 months

Email

15 **Personal use**: School email account should be used for work purposes only however the School permits the incidental use of its email system subject to certain conditions set out below to send personal emails. This permission must not be overused or abused.

The School may monitor your use of the email system, please see paragraphs 23 to 27 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

Use of Email: 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.

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.

If staff send an email in error that contains the personal information of another person, they must inform the IT Department immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

16 **Status**: Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published eg. emails may be disclosed during a subject access request.

17 **Unacceptable use**:

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

Unacceptable use of the school's ICT facilities includes:

- 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

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

18 **Legal proceedings**: You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19 **Jokes**: Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

20 **Contracts**: Contractual commitments via an email correspondence are not allowed without the prior authorisation of the Bursar.

22 **Disclaimer**: All correspondence by email should contain the School's disclaimer.

22 **Data protection disclosures**: Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a Subject Access Request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). Staff must be aware that anything they put in an email is potentially disclosable.

Monitoring

23 The School reserves the right to monitor and access its IT system for purposes connected with the operation of the School. The School IT system includes, but not limited to, any hardware, software, email account, computer, device or telephone provided by the School or used for School business. Staff should be aware that the School will monitor the contents of a communication (such as the contents of an email).

24 The purposes of such monitoring and accessing include:

24.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

24.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

24.3 to safeguard and promote the welfare of children and provide them with safe environment to learn.

25 Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

26 The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

27 The monitoring is carried out by Smoothwall and reported to the Deputy Head. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Head and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.