Policy Owner	Maureen Foakes
Approving Body	Board of Governors
Date Approved	February 2020
Effective Date	February 2020
Review date	February 2023

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 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 Network Manager. 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. Do not choose a password which is so complex that it's difficult to remember without writing it down. 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.

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;

8.3 acceptable use of IT policy for pupils

8.4 online safety 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 inappropriate purposes (as described in section 11 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 via 3G or 4G 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**: The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. 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.

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 generally.

17 **Inappropriate use**: Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

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 through the email system. They could cause offence.

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

21 **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 regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes 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.

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.

I confirm that I have read the Staff IT Acceptable Use Policy above.

Signed…….

Name…….. Date……