IT Acceptable Use Policy for Staff & Volunteers

Queen's College, Taunton

August 2020 (V3)

IT Acceptable Use Policy for Staff & Volunteers

1 **Introduction:** This policy sets out the requirements with which you must comply when using the School's email and internet services including the use of mobile technology on School premises or otherwise in the course of your employment (this includes mobile data access) whether on a School or personal device. This policy also applies to the use of email and internet services off school premises if the use involves any member of the School community or where the culture or reputation of the School are put at risk. Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

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

3 **Programs, Applications and Apps:** Programs, applications and apps must not be downloaded, installed or removed without permission from the IT Department. Licence terms must be adhered to at all times to ensure that the school is not liable. Software that is purchased from personal accounts cannot be installed on school computers or devices. You also must not purchase software on the school's behalf. Any and all software purchases must be made through the IT Department where it can be checked for suitability and compatibility with devices and the school's technological environment.

4 **Viruses and Malware:** You should be aware of the potential damage that can be caused by computer viruses and malware. You must not introduce or operate any programs or data (including games) or open suspicious emails without permission from the IT Department.

5 **Passwords:** Passwords protect the School's network and computer system. They should not be obvious, for example a family name or birthdays, and should be a mix of uppercase and lowercase, numbers and special characters (e.g. #, &, !) and a minimum of eight characters. You should not let anyone else know your password. If you believe that someone knows your password you must change it immediately by contacting the IT Department or e-mailing password@queenscollege.org.uk. You should not attempt to gain unauthorised access to anyone else's technology (whether computer or mobile device) or to confidential information which you are not authorised to access.

6 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action to secure your computer 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 / Designated Safeguarding Lead. For example, if you have a concern about IT security or pupils accessing inappropriate material.

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

7.1 Code of Conduct Policy;

7.2 Data Protection Policy;

7.3 Social Media Policy;

7.4 IT Acceptable Use Policy for Pupils and;

7.5 Online Safety Policy.

Internet

8 **Downloading:** Downloading of any program, file or application which is not specifically related to your job is strictly prohibited.

9 **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 10 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.

10 **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.

11 **Contracts:** You are not permitted to enter into any contract or subscription on the internet on behalf the School, without specific permission from the Head. This also applies to software/application purchases which cannot be made without approval from the IT Department.

12 **Retention periods**: the School keeps a record of staff browsing histories for a minimum period of 6 months.

Email

13 **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 21 - 23 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.

14 **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.

15 **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.

16 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy exists in archived form for a minimum of six months.

17 **Jokes:** Trivial messages and jokes should not be sent or forwarded via email. They could cause the School's IT system to suffer delays or cause offence even if none is meant.

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

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

20 **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 the Data Protection Act 2018. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **As such staff must be aware that anything they put in an email is potentially disclosable.**

Monitoring

21 **Monitoring:** Staff acknowledge and agree that the School regularly monitors and accesses the School IT system for purposes connected with the operation of the School. 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). The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School may also monitor staff use of the School telephone system and voicemail messages. The purposes of such monitoring and accessing include:

21.1 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

21.2 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.

22 The monitoring is carried out by the IT Manager. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Deputy Head / Designated Safeguarding Lead / Head and this may result in disciplinary action. In exceptional circumstances concerns may need to be referred to external agencies such as the Police.

23 Before engaging in such activities the School will undertake a privacy impact assessment (PIA) to help the School decide whether the monitoring is justified in the circumstances or whether there are less intrusive means of achieving the same aim. A PIA should in particular identify the purposes behind the monitoring, consider the likely adverse impact of the monitoring as well as alternatives, take account of the obligations that arise from the monitoring and set out the School's decision on whether or not the monitoring is justified.

Effective date of the policy	31st August 2020
SLG Responsible Member	Andrew Free, Deputy Head

Authorised by	Board of Governors
Signed	Mark Edwards, **Chair of Governors**
Date	31St August 2020