HORRIS HILL
FOUNDED 1888

IT Acceptable Use Policy (Staff)

Policy reviewed:	**September 2021**
Policy approval:	**Reviewed by SJB Autumn term 2021** **For approval by Forfar Education**
Date of next review:	**Autumn term 2022**

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 **e**mail 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 (to include the use of Whatsapp and other technology based communications); and

1.4 any hardware (such as PCs, laptops, printers or mobile phones) or software provided by, or made available by the School, or otherwise used in connection with your job.

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

2 **Training:** Induction training for new staff includes training on the School's online safety strategy. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sharing nudes and semi-nudes images and/or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes.

3. **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. 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. You should not remove equipment or information from the School's premises without appropriate approval. If approval has been given, you should take precautions to protect the computer media and equipment when carrying it outside the School's premises (eg leaving a laptop unattended or on display in a car such that it would encourage an opportunistic theft).

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 not relevant to your work (including computer games) or open suspicious emails without permission from the Bursar. You must not disable antivirus protection provided on any computer, except where required for a specific purpose eg troubleshooting, after which it must be re-enabled immediately afterwards.

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. You are responsible for the use and protection of the user credentials provided to you by the School. 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 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.

5.4 You should not attempt to access any computer system to which you have not been given access or use anyone else's user account and password to access the School's systems unless required to do so as part of your job or if permission has been given by the Headmaster or Bursar.

5.5 You should not attempt to bypass or subvert system security controls or use them for any purpose other than that intended, except when permission has been given by the Headmaster or Bursar.

5.6 You should protect any confidential material sent, received, stored or processed, including both electronic and paper copies.

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 Headmaster or Bursar. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Online Platforms:** The School uses online platforms such as Zoom and G Suite to support and facilitate learning and pupil engagement. You must make sure that you follow the School's policies, procedures and instructions notified to you in respect of such platforms.

9 **Remote Access to School IT Systems:** Staff may be authorised to access the school network remotely by 'Remote Desktop Services' and can access the e-mail system by 'Outlook Web Access'. Staff are expected to maintain suitable anti-virus protection on personal equipment used for this purpose and should not store school data on non-school equipment.

All school policies and procedures relating to the use of IT are equally applicable when that use is by remote means.

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

9.1 Safeguarding and Child Protection Policy and Procedures

9.2 Staff Code of Conduct;

9.3 Data Protection policy for Staff;

9.4 Acceptable Use policy for Pupils; and

9.5 Online Safety Policy.

Internet

11 **Downloading:** Downloading of any programme or file which is not specifically related to our job is strictly prohibited.

12 **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 12 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 Headmaster.

13 **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 Headmaster whilst allegations of unsuitable use are investigated by the School.

14 **Location services:** [Intentional deletion].

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

16 **Retention periods**: the School keeps a record of staff browsing histories for a period of [period to be inserted following discussion with Connect Systems].

Email and other technology based communications

17 **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. 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 23-27 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.

18 **Group communications**: Where necessary, the School permits the use of group communications, for example with the use of email groups of Whatsapp groups. When using such groups, staff should:

18.1 never share confidential personal details, particularly pupil or parent information;

18.2 not include pupils or parents in the group;

18.3 be mindful of the School's Dignity at Work Policy, Social Media Policy, Online Safety Policy and Staff Code of Conduct;

18.4 have no expectation that messages sent will remain private, for example the messages may be disclosable under a subject access request or may be used by the School in formal processes if they evidence misconduct or performance concerns; and

18.5 not use group messaging as a means of formal communication when an audit trail is needed.

19 **Status:** Email and other technology based communications (to include text or iMessage, Whatsapp) should be treated in the same way as any other form of written communication. Anything that is written in an email or other technology based communications is treated in the same way as any form of writing. You should not include anything in an email or other technology based communication which is not appropriate to be published generally.

20 **Inappropriate use:** Any email message or other technology based communication 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.

21 **Legal proceedings:** You should be aware that emails, texts and other messages 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.

22 **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.

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

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

25 **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

26 **Monitoring:** 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. The School may also monitor staff use of the School telephone system (by extension number and destination). Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).

27 The purposes of such monitoring and accessing include:

27.1 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

27.2 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.

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

29 Staff should be mindful that when websites are visited, cookies, tags or other web beacons may enable the site owner to identify and monitor visitors.

30 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).

31 The monitoring is carried out by the Designated Safeguarding Lead and the School's ICT provider as requested by the Headmaster or Bursar. If anything of concern is revealed as a result of such monitoring then this information must be shared with the Headmaster and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.