Acceptable use of IT agreement for staff

1. Training

Induction training for new staff includes training on the School's online safety approach and policy. Ongoing staff developmental training; includes training on technology safety, together with specific safeguarding issues; including the sharing of nude and semi-nude images and/or videos, cyberbullying, radicalisation and dealing with harmful online challenges, and online hoaxes.

2. Property

You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the IT coordinator/IT Support (B Hibbert/D Cowen). You should not use the School's computers unless you are competent to do so and should ask for training if you need it. If you would like any IT equipment relocated/changed, please contact the IT Support Team (B Hibbert/D Cowen). This must NOT be carried out by yourselves, due to Health and Safety reasons.

3. Viruses and Malicious Code

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

3.1 Vigilance Against Spam and Hoax Emails

In order to protect the security and integrity of our school's digital environment, all employees are required to exercise heightened vigilance when handling incoming emails. Be cautious of unsolicited emails, especially those that request personal or financial information, contain suspicious attachments, or encourage urgent actions. Phishing attempts, hoaxes and malware often disguise themselves as legitimate communication. If you receive an email that seems suspicious or too good to be true, do not click on any links, download attachments, or respond to the sender. Instead, report the email to the IT Support Team immediately for verification. Always verify the authenticity of requests, especially those involving sensitive data, before taking any action.

4. Passwords

Passwords protect the School's network and computer system. They should not be obvious, for example a family name or birthdays, should be a minimum of 14 characters long, include a mix of uppercase and lowercase letters, numbers and special characters (e.g. #, &, !). You should not let anyone else know your password. **If you believe that someone knows your password, you must change it immediately.** Forced password changes take place regularly and your updated password should not be similar to the previous one (for example do not change your password by just adding a number each time, e.g. orchard1, orchard2, orchard3 etc). You should not attempt to gain unauthorised access to anyone else's computer or to confidential information which you are not authorised to access. The School will require several password changes over the course of each academic year. Passwords should not be written down.

5. 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. A shortcut to this on a Windows PC is the Windows Key + L. To lock your Chromebook screen, press the Launcher key (or Search key) + L simultaneously. The Launcher key is the one with a magnifying glass, located where the Caps Lock key usually is on a standard keyboard. Alternatively, you can click the time in the bottom-right corner and then select the Lock icon. If your PC is in a potentially shared area such as a classroom or an office, then if you are likely to leave your workstation for an extended period of time, you should as a matter of courtesy log out of the workstation/Chromebook.

6. **Concerns**

You have a duty to report any concerns about the use of IT at the school to the DSL/Deputy Head. For example, if you have concerns about IT security or pupils accessing inappropriate material.

7. **Online Platforms**

The School uses online platforms to support its routine activity. You must make sure that you follow the School's policies, procedures and instructions notified to you in respect of such platforms.

8. **Other policies**

This policy should be read alongside the following:

8.1 Staff Handbook
8.2 E-Safety Policy;
8.3 Data Protection Policy for Staff;
8.4 Policy on the Safe and Acceptable Use of ICT for Pupils.

Internet

9. Downloading

Downloading of any programme or file is strictly prohibited. Anything related to your work environment would be carried out by the IT Support Team.

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 and in the staff room. 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 within 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 at the discretion of the Head. Any personal use of a School device is subject to the School's permission in accordance with its policies. If you do use a School device for personal reasons, please be aware that such personal use may be monitored.

10. Personal Devices

Personal devices will not be permitted access to the school's Wi-Fi network. During lunch and break periods, staff members may use their personal devices exclusively within the staff room and must utilise their own mobile data for internet access. Personal devices should not be visible and should be switched off during working hours.

11. Device Syncing

Personal use of School devices may result in the School device syncing with your personal accounts and devices, for example, if you log into a personal account on the School device. This could, for example, result in private browsing history and personal information transferring from a personal device to a School device, and therefore becoming subject to monitoring by the School. You may be able to prevent this by turning off device syncing on your personal device. This is your responsibility and the School has no control over automatic syncing. If in doubt, do not use a School device for personal reasons.

12. 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, 4G or 5G 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.

13. 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 very strongly discouraged.

14. Contracts

You are not permitted to enter into any contract or subscription on the internet on behalf of the School, without specific written permission from the SLT/ IT Support Team. This applies both to "free" and paid for contracts, subscriptions and Apps.

15. Internet Browsing

The School keeps a record of staff browsing histories and holds an email archive. Parents who also have one or more children at the School should be especially aware of this detail.

15.1 Smoothwall

Please refer to the Smoothwall Policy with regards to how it is utilised within our School environment.

Email

16. Personal use

The School does not permit the incidental use of its work email systems to send personal emails. Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 29, 30 and 31 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. There should not be an expectation of privacy in cases where staff are using School systems for private matters.

17.Use of personal devices or accounts for School business

The School accepts you may use your personal devices, social media or messaging services to maintain social contact with colleagues as part of your private life. Where contact with colleagues includes both personal and professional matters, there is a risk of blurring boundaries as to what devices and platforms should be used for what type of contact. The School expects you to exercise your professional judgement in order to ensure all communication is appropriate and professional at all times. In the rare event you might need to contact a colleague about a work-related matter using a personal device or personal social media, you must keep any such messages brief and professional, and must not include any identifying and/or sensitive information. For example, you could send a message to a colleague's personal WhatsApp account asking them to check their School email account without providing any further information. All further communication should then take place using the appropriate School platforms.

18. Group communications

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

- never share confidential personal details, particularly pupil or parent information; not include pupils or parents in the group;
- be mindful of the School's Social Media Policy as in staff manual; 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 not use group messaging as a means of formal communication when an audit trail is needed.

19. Status

Email and other technology based communications (including but not limited to 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 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.

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 equality, diversity and inclusion policy), or defamatory is not permitted. Use of the email system in this way constitutes a breach of the School's anti-bullying policy and may constitute 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. This is the case regardless of whether the communication has taken place using the School's equipment and systems, or your own equipment and social media/messaging service. Even if messages are deleted, a copy may exist on a back-up system or other storage area. 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.

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.

23. Large files

Any large non-work related files should not be sent using the email system. They could cause the School's IT system to suffer delays and / or damage. Colleagues should use links to files stored in facilities such as Google Drive.

24. Contracts

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

25. Disclaimer

All correspondence by email should contain the School's disclaimer.

26. 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 General Data Protection Regulation 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.** This is the case regardless of whether the communication has taken place using the School's equipment and systems, or your own equipment and social media/messaging service.

27. Artificial Intelligence

The School wishes to support staff to use AI as a learning tool, in order to support pupils' learning, to boost productivity, and to help manage workloads efficiently and effectively. You are permitted to use AI software at work and for work purposes. If you use AI technology at work or for work purposes, you must do so professionally at all times. This means that you may use AI as a tool to help you perform your role but must not use it to cut corners. You must not input any confidential information into free generative AI software such as ChatGPT. You must also check any output generated by AI technology before adapting it for your final use.

28. 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 purposes of such monitoring and accessing include:

28.1 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 or redirected in case any urgent emails are received; and

28.2 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.

28.3 to diagnose reported faults within the School IT network.

28.4 Part of the monitoring of School systems will include phishing simulations which will take place as required, the purpose of these simulations is to ensure that staff maintain vigilance in the face of cyber attacks. Those that repeatedly fail the phishing simulations may be required to undertake additional training.

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 monitoring is carried out by the Head, DSL and IT Support Team. 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.

Updated September 2025