Information Security Policy

Owner:	**Data Compliance Lead**	**Date Reviewed:**	**July 2023**
Review Period:	**1 Year**	**Next Review Date:**	**July 2024**

CONTENTS

1. ABOUT THIS POLICY

1.1 Our IT and communications systems ('**ITC systems**') are used to promote effective communication and working practices within Prep Schools Trust (the "Trust") and our schools. This policy outlines the standards you must observe when using ITC systems and the circumstances in which we will monitor your use of ITC systems. It also covers practices and organisational measures required in relation to all manual files containing personal data.

1.2 In this policy, the term 'school(s)' means Barfield, Chandlings Prep, Cothill House, Kitebrook Preparatory and Mowden Hall. For the avoidance of doubt, the Trust is the data controller for all the schools governed and administered by the Trust and this policy is therefore intended to be written on behalf of all the schools in the Trust.

1.3 This policy applies to our staff, including employees, trustees, interns, volunteers, consultants, external contractors, temporary workers, agency workers and casual workers and anyone who has access to our ITC systems.

1.4 Misuse of ITC systems or loss or misuse of personal data contained in manual files can damage our reputation and have serious legal and financial consequences for the Trust and our schools. Breach of this policy may therefore be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to dismissal.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

1.6 The ITC system contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy and related policies, in particular the Bring Your Own Device Policy and Working from Home policy.

2. PERSONNEL RESPONSIBLE FOR THE POLICY

2.1 The Trust Chief Operating Officer has overall responsibility for ensuring the effective and fair operation of this policy and for ensuring compliance with the relevant laws.

2.2 Trust Technical Support will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

3. EQUIPMENT SECURITY AND PASSWORDS

3.1 You are responsible for the security of the equipment allocated to or used by you in connection with your role at the school or Trust, and must not allow it to be used by anyone in breach of this policy.

3.2 You are responsible for the security of any device used by you (e.g. computer or mobile phone). You should lock your device or log off when not in use, to prevent unauthorised users from accessing the system in your absence.

3.3 You should not allow any unauthorised person to use any school/Trust device.

3.4 Desktop computers and cabling for telephones or computer equipment should not be moved or tampered with without first consulting Trust Technical Support

3.5 You should use strong passwords on all IT equipment, particularly devices or data storage disks/devices that you take out of the office. You must keep your passwords confidential, change them regularly and do not store them in plain text. You must not use another person's username and password or allow anyone else to log on using your username and password.

3.6 On the termination of employment (for any reason), you must return any IT equipment and documents. Your Google account will be suspended and passwords reset.

3.7 If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Any equipment where personal data is likely to be stored or used for transfer purposes, must be encrypted (whole disk encryption) and password protected (with a strong password required at start up and also after a period of inactivity) to ensure that confidential data is protected in the event of loss or theft. You should not use the school/Trust's equipment in a place where documents may be read by third parties, for example, passengers on public transport. Whenever appropriate, you should use privacy screens to ensure that the information is not visible to other people.

4. SYSTEMS AND DATA SECURITY

4.1 You must not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2 You must not download or install software from external sources without authorisation from Trust Technical Support. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by Trust Technical Support before they are downloaded. If in doubt, staff should seek advice from the IT Department.

4.3 You must not attach any device or equipment to our systems without authorisation from Trust Technical Support. This includes any USB flash drive, tablet, smartphone or other similar devices, whether connected via the USB port, Bluetooth or in any other way.

4.4 We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email that appears suspicious (for example, if it contains a file whose name ends in .exe). Inform Trust Technical Support immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

4.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

4.6 You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. Personal data should not be processed from an unsecured physical environment, such as third party unsecured WiFi networks (e.g. a mobile hot-spot including free Wi-Fi provided in airports, hotels, coffee shops, etc.). School/Trust devices should only connect to an unsecured third party WiFi network when absolutely necessary and provided that a secure web session is put in place to protect the data.

5. EMAIL

5.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as

professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

5.2 Emails to pupils should always be written professionally and signed off in an appropriate manner.

5.3 You should access your emails during a working day, stay in touch by remote access when travelling in connection with business, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked "high priority" within 24 hours.

5.4 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate and unprofessional emails. Anyone who feels that they are being or have been harassed or bullied, or is offended by material received from a colleague via email, should inform the Trust HR Manager.

5.5 You should 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. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

5.6 Email messages are required to be disclosed in legal or regulatory proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software and disclosable.

5.7 In general, you should not:

(a) send, forward or read private emails at work or forward work emails or the school/Trust's documents to your private address;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

(d) sell or advertise using our ITC systems or broadcast messages about lost property, sponsorship or charitable appeals.

(e) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

(f) download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another person's email address (unless authorised) or under an assumed name;

(h) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

5.7 If you are sending personal, sensitive and/or confidential information via email, you should ensure that:

(i) personal, sensitive and/or confidential information should be contained in an attachment, which should be encrypted, and/or password-protected, where appropriate.

(j) any password or key must be sent separately.

(k) before sending an email containing personal, sensitive and/or confidential information, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent.

(l) mark emails as 'Confidential' or 'Confidential and privileged', as appropriate and do not refer to the confidential information in the subject of the email.

(m) to avoid unauthorised disclosure of email addresses when emailing multiple recipients, use Bcc function where appropriate.

5.8 If you receive an email in error you should inform the sender immediately.

5.9 Do not use your own personal email account to send or receive an email for the purposes of our business. Only use the email account we have provided for you.

6. USING THE INTERNET

6.1 Internet access is provided primarily for business purposes related to the running of the school and Trust.

6.2 When a website is visited, files such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in section 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under section 9.

6.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

6.4 Except as authorised in the proper performance of your duties, you should not under any circumstances use our ITC systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

7. PERSONAL USE OF OUR SYSTEMS

7.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

7.2 Personal use must meet the following conditions:

(a) Use must be minimal and take place substantially out of normal working hours

(b) Use must not interfere with business or office commitments.

(c) Use must not commit us to any marginal costs.

(d) Use must comply with this policy (see in particular sections 5 and 6) and our other policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy, Disciplinary Procedure.

7.3 You should be aware that personal use of our systems may be monitored (see section 8) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see section

9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

8. MONITORING

8.1 Our systems enable us to monitor all ITC systems usage (including internet usage and network traffic, files accessed, the use of phone, email systems, collaboration software, video conferencing software and any messaging apps used for work), subject to sections 8.2 - 8.4 below.

8.2 Systems logs and audit trails are in place and user logs are regularly reviewed. The specific content of any communications and files will not be monitored unless there is business need or a suspicion of improper use. The school/Trust has the right to access and review the content of any communication or file within the school/Trust's ITC systems (including those marked 'personal') and to process personal data in this context, if there is a suspicion of improper use of the school/Trust's ITC systems. emails and other communications and files marked 'personal' might also need to be accessed to the extent that IT support cannot avoid accessing such information while fixing a problem.

8.3 The ability to monitor other colleagues' use of the school/Trust's ITC systems and access to information about other colleagues' activities or communications is restricted to nominated employees on 'needs to know' basis. In the case of a specific allegation of misconduct or misuse of the school/Trust's ITC systems, such allegation should be notified to the relevant line manager and any monitoring activities or access to content need to be authorised in compliance with this policy.

8.4 We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the operation of the school/Trust, including for the following purposes (this list is not exhaustive):

(a) to monitor whether use of the email system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing;

(d) to comply with any legal obligation.

9. PROHIBITED USE OF OUR SYSTEMS

9.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our ITC systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) Pornographic material (that is, writing, pictures, films and video clips).

(b) Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to the school/Trust community.

(c) A false and defamatory statement about any person or organisation.

(d) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others

(e) Confidential information about us, the operation of the school/Trust, any of our staff, and the wider school/Trust community (except as authorised in the proper performance of your duties).

(f) Unauthorised software.

(g) Any other statement which is likely to create any criminal or civil liability (for you or us).

(h) Music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

9.2 Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

10. HARD COPY DOCUMENTS

Hard copy documents should be stored securely. Access to school/Trust documents containing confidential data and personal data should be restricted to those who need to access the relevant information to fulfil their roles. Access should be protected through appropriate access controls, to prevent access by any unauthorised person and where appropriate, all access should be logged.

11. ACKNOWLEDGEMENT OF YOUR DUTIES

All staff and anyone else who has access to our ITC systems are required to read this policy on starting their employment with the Trust and confirm their understanding and acceptance of this policy during their induction to their line-manager.