IT and Communications Policy

About this policy

8.5.1 Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

This policy applies to all ODBF employees, contract/temporary staff and any other individuals with access to the ODBF's IT systems.

8.5.2 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Equipment security and passwords

8.5.3 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly, at least every 3 months. Your password should be a hard-to-guess combination, at least 8 characters (including upper and lower case letters and a numerical digit), and should not include your name. A strong numerical passcode, that is not easy to guess, should be set on mobile phones or tablets used for work purposes.

8.5.4 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password, without the permission of IT and your Departmental Head.

8.5.5 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day

Systems and data security

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

8.5.7 You must not download or install software or any application from external sources without authorisation from your line manager and the IT department. Downloading unauthorised software or apps may interfere with our systems and may introduce viruses or other malware.

8.5.8 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an email looks suspicious do not reply to it, open any attachments or click any links in it.

8.5.9 Inform your line manager immediately if you suspect your computer may have a virus.

8.5.10 Networked drives (R: drive and U: drive) and Microsoft OneDrive are provided for you to save documents used in the performance of your role (files saved in these locations are automatically backed up). To maintain the highest levels of security and resilience it is recommended that documents are not saved onto your local computer hard disc drive. Other cloud storage solutions, such as Dropbox, are not recommended. Documents should only be stored onto a USB device where necessary. Sensitive information stored should always be password protected. If you require regular use of a USB storage device, you should consider encrypting it.

Use of your own devices

8.5.11 If you access your work emails or data on a personal device (PC, tablet, etc.), documents should not be stored on that device. We recommend you access Office 365 using a web browser, which provides access to your work without storing files permanently on the local device. See the Information Security policy for more details on the use of your own devices for work purposes.

E-mail

8.5.12 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

8.5.13 Remember that e-mails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

8.5.14 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

8.5.15 You should not: (a) send or forward private e-mails at work which you would not want a third party to read; (b) send or forward chain mail, junk mail, cartoons, jokes or gossip; (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or (d) send messages from another person's e-mail address (unless authorised) or under an assumed name.

8.5.16 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our organisation. Only use the e-mail account we have provided for you.

Using the internet

8.5.17 Internet access is provided for organisation purposes. Occasional personal use may be permitted as set out in paragraph 8.5.20 and 8.5.21

8.5.18 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive or immoral. Even web content that is legal in the UK may 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. If such access is necessary for work purposes, written approval must be granted in advance by your Head of Department, in consultation with the IT team.

8.5.19 We may block or restrict access to some websites at our discretion.

Personal use of our systems

8.5.20 We permit the occasional use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. 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.
8.5.21 Personal use must meet the following conditions: (a) it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work); ; (b) it must not affect your work or interfere with the organisation; (c) it must not commit us to any marginal costs; and (d) it must comply with our policies including the Equal Opportunities Policy, Antiharassment and Bullying Policy, Data Protection Policy, Social Media and Disciplinary Procedure.

Monitoring
8.5.22 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For organisational reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.
8.5.23 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the organisation, including for the following purposes (this list is not exhaustive): (a) to monitor whether the use of the e-mail 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; or (d) to comply with any legal obligation.
8.5.24 Only the Diocesan Secretary has the authority to approve action under 8.5.23 above

Prohibited use of our systems
8.5.25 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.
8.5.26 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive): (a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature); (b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients; (c) a false and defamatory statement about any person or organisation;
(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy); (e) confidential information about us or any of our staff or clients (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); or (h) music or video files or other material in breach of copyright.

Lost or stolen equipment
8.5.27 Any lost or stolen IT equipment, either issued to you by ODBF or a personal device that you use to access ODBF's data and systems, must be reported to our IT provider and your line manager as soon as possible, even if this is outside of normal office hours. Immediate notification is imperative, since this constitutes a data breach under data protection law. IT can be contacted on: 01793 688 596.
8.5.28 Once you have discovered your device is missing you should use an alternative device to log on to Office 365 (using your computer login credentials) and change your password immediately, in case your account password has been compromised. IT will initiate a remote wipe of any mobile device to remove all data.

June 2026