TEDI-LONDON - IT ACCEPTABLE USE POLICY

Summary	Policy for acceptable use of TEDI-London IT services.		
Policy Owner	Head of Technology		
Policy Sponsor	Chief Operating Officer (COO)		
Policy applies to	All staff, students, contractors and consultants.		
Relevant Legislation and Policies	• Data Protection Act (2018) • Counter-Terrorism and Security Act (2015) • Regulation of Investigatory Powers Act 2000 • Freedom of Information Act 2000 • Human Rights Act 1998 • Computer Misuse Act 1990 • PREVENT Duty guidance (2015) • Data Protection Policy • Privacy notice • Safeguarding • Dignity at Work		
Equality impact assessment completed	No		
Version	1.2		
Approved by	Policy Working Group	**Approval date**	01/08/2023
Date of implementation	18/09/2020	**Date of next formal review**	08/2024

DOCUMENT CONTROL

Date	Version	Action	Amendments
09/2020	1	Policy created	n/a
01/2021	1.1	Reviewed	Replace references to Microsoft Cloud with One Drive / Sharepoint
07/2023	1.2	Reviewed	Amended roles for approval and ownership, additional wording about cybersecurity incidents, account permissions and password guidance.

Contents

1. INTRODUCTION

1.1 This Policy outlines the key responsibilities and required behaviour of all staff and students using TEDI-London's IT systems.

1.2 You are required to read, understand and adhere to this Policy.

1.3 All IT resources provided are the property of TEDI-London and must be used or accessed in accordance with this policy.

2. POLICY STATEMENT

2.1 You are required to adopt the practices outlined in this policy to ensure the security, integrity and protection of the information held by TEDI-London.

2.2 This Policy adheres to UK legislation, including:

- Data Protection Act 2018
- Counter-Terrorism and Security Act 2015
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- PREVENT Duty guidance 2015

2.3 This Policy includes Information security guidance and should be read alongside our Policies for:

- Data Protection Policy
- Privacy notice
- Safeguarding
- Dignity at Work Policy

3. SCOPE

3.1 This Policy applies to all employees, students, consultants and contractors of TEDI-London with access to TEDI-London IT.

4. TEDI-LONDON CREDENTIALS

4.1 You must take all reasonable precautions to safeguard your usernames, passwords, and any other IT credentials. You must not allow anyone else to use your IT credentials.

4.2 You must not attempt to obtain or use anyone else's credentials.

4.3 You must not impersonate someone else or otherwise disguise their identity when using the IT facilities.

4.4 Passwords must conform to guidance regarding length and complexity established by IT.

4.5 In order to access some IT services, we require you to authenticate your identity through Multi-Factor Authentication (MFA) technology. To access those systems where MFA technology has been enabled, you will be required to provide unique information sent to you via an independent method such as an authenticator application, SMS message to a pre-registered mobile device or a similar alternative method supported by TEDI-London, in addition to your username and password.

5. CONFIDENTIALITY

5.1 You must take all reasonable steps to safeguard personal, confidential, or sensitive information, and must be aware of and observe the requirements of our Data Protection Policy.

5.2 You should not export data from our systems, but if this is unavoidable, you must ensure that any data exported is handled in such a way as to maintain the confidentiality and security of that data.

6. E-MAIL AND COLLBORATIVE TOOLS

6.1 This section covers the use of TEDI-London email accounts. It also applies to other collaborative tools, such as Microsoft Teams, Microsoft Groups, and shared mailboxes.

6.2 Only TEDI-London email accounts must be used to conduct TEDI-London business.

6.3 You must not auto-forward/redirect your TEDI-London email to a personal or other account (e.g. a Hotmail or Gmail account) or account provided by another organisation.

6.4 Assigned TEDI-London email addresses are for the sole use of the individual user. Access to another user's mailbox without the user's permission is prohibited (unless in accordance with Section 13).

6.5 You must take reasonable measures to prevent the transmission of viruses and ransomware attacks, such as not opening email attachments received from unsolicited sources. You must report all suspicious email messages arriving in your Inbox to IT Service Desk.

7. INFORMATION SECURITY

7.1 Information security measures protect information from a wide range of threats and safeguard information. Our information security measures are based on the following principles:

- Confidentiality to ensure our information is not made available or disclosed to people or organisations who do not have authorisation to see it.
- Integrity to ensure our information is complete and error free.
- Availability to ensure our information and associated services are available to authorised users when required.

7.2 We will:

- Maintain a secure environment in which to create, use and store information.
- Protect all confidential, restricted, and personal/sensitive personal information from unauthorised use and disclosure.
- Comply with regulations and laws to avoid any penalties or fines for non-compliance.
- Assign account permissions based on the Principle of Least Privilege access (PoLP) – with users only having access to data and applications required for their job. There are no local admin permissions on TEDI-London devices

7.3 You must immediately report any suspected breaches, cyber-attacks or security related issues to IT Services and, in the case of a breach that may compromise personal data, must also notify the Data Protection Officer (currently the Director of Resources) immediately.

7.4 Any storage device used for commercially sensitive or personal data must be appropriately encrypted. Please ask IT Services for advice if you are not sure if your device meets the standards required.

7.5 We manage your corporate devices with software that can enable us to disable or wipe the device remotely. If you lose or have a device stolen you must report this to IT services as soon as possible so the necessary steps can be taken.

7.6 You can use your own device (BYOD) to access the TEDI-London IT environment. We have restricted access to only the more recent operating systems and devices to help ensure information security. We will manage the Microsoft apps on your personal device with corporate software. This enables us to delete the data in the applications or disable access remotely.

Please ensure you comply with the guidance provided for storing of data and inform IT services if you think your device is lost or stolen.

7.7 Any member of staff working remotely is responsible for ensuring that they work securely and protect both information and TEDI-London-owned equipment from loss, damage or unauthorised access. All practices and constraints outlined in this policy apply to all users of IT services when working remotely.

7.8 When working from any location you should ensure that the screen lock is engaged on your device if you leave it unattended. If you regularly work in public locations or regularly deal with sensitive information, you should consider the use of a privacy screen.

8. TEDI-LONDON OWNED IT EQUIPMENT

8.1 Users of TEDI-London owned equipment (including mobile devices) are responsible for that equipment. They must take all reasonable steps to protect and secure their device and any data stored on it, as outlined in this policy, associated policies and procedures.

8.2 You must manage the consumption of data on your mobile devices to remain as much as possible within the limits set and prevent additional costs being incurred.

8.3 In normal circumstances, you must return your computing equipment when they leave TEDI-London.

8.4 Use of a mobile device by anyone other than the named user is prohibited.

9. USE OF ADDITONAL TECHNOLOGIES

9.1 You must not create or build your own solutions for your business or academic processes without consulting IT for advice and support.

9.2 Purchase and installation of hardware or software that connects to TEDI-London's system(s) is not permitted without prior consultation with IT Services.

9.3 Use of supportive technology, such as those tools available through Office 365 (e.g. Power Automate, Microsoft Stream), is bound by the practices and constraints outlined in this policy, associated procedures and any licensing or contractual agreements.

10. SOFTWARE LICENSES

10.1 You must adhere to any licence conditions when using software procured by TEDI-London.

11. UNACCEPTABLE USE

11.1 The following are examples of unacceptable use. The list is not exhaustive.

- Creating, transmitting, storing, or displaying insulting, indecent or obscene material.
- Accessing or using TEDI-London IT for malicious reasons such as cyber-attacks, data theft or systems interference.
- Accessing, storing, transmitting or similar, online material which would usually be considered 'inappropriate' in a work environment such as pornography, whether legal or otherwise. This may include material considered to create a hostile working environment
- Creating, transmitting, or displaying material that deliberately and unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the

grounds of race, ethnicity, gender, sexual orientation, marital status, age, and disability, political or religious beliefs.
- Creating, transmitting or displaying defamatory material.
- Obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper authority.
- Contravening the policy of a third-party company with which the TEDI-London holds a contract for IT services.
- Creating or transmitting material with the intent to defraud.
- Creating or transmitting material or using university systems for commercial purposes unrelated to the interests of the university.
- Causing annoyance or inconvenience, e.g. sending unsolicited email chain letters, unauthorised bulk email (spam), which is unrelated to the legitimate business of TEDI-London.
- Sharing information when not authorised to do so (especially commercially sensitive, personal and sensitive personal data).

11.2 We have a statutory duty, under the Counter-Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. You must not create, download, store or transmit unlawful material, or material that can reasonably be considered to be indecent, offensive, defamatory, threatening, discriminatory or extremist. We reserve the right to block or monitor access to such material.

11.3 Intentionally interfering with the normal operation of the network, including the spreading of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

11.4 Exceptions needed to this policy (for example, for purposes of properly supervised and lawful research) should be raised with IT Services.

12. PERSONAL USE

12.1 A reasonable level of personal use of IT devices and systems is permissible. Personal use must not interfere with TEDI-London business or the performance of your duties.

12.2 You must ensure, particularly, that their personal use of devices does not lead to consumption of data beyond set limits.

13. MONITORING AND IT ACCESS.

13.1 We monitor and record the use of our IT facilities for various purposes including:

- The effective and efficient planning and operation of IT facilities.
- Detection and prevention of infringement of this policy, related procedures and relevant legislation.
- Investigation of alleged misconduct.
- Compliance with lawful requests for information from government and law enforcement agencies.

13.2 Where personal data is being processed as part of these activities, the GDPR lawful basis is that such monitoring is necessary for TEDI-London's legitimate interests, and these interests override the impacts on the users.

13.3 The Head of Technology, on the authorisation of the Chief Executive Officer, Chief Operating Officer, or People Partner, may grant access to your account for any of the reasons noted in 13.1 or to permit ongoing operations in the event of your death, incapacity, suspension, dismissal, departure or long-term absence.

13.4 Before authorisation is granted, a Data Protection Impact Assessment must be carried out to identify the purpose of the access, the adverse impact on individuals, whether there are less intrusive means of achieving the aim, and whether the access is justified.

14. CONSEQUENCES OF BREACHING THIS POLICY

14.1 Any breaches of this policy may be treated as a disciplinary offence and may constitute an offence under data protection legislation or regulation as outlined in the GDPR Policy

ANNEXE 1 TEDI-LONDON DOCUMENT MANAGEMENT PROCEDURE

TEDI-London promotes a cloud first, Microsoft only approach to document storage. Microsoft security and encryption features means our data is well protected.

Please ensure that all documents are stored as applicable on:

- OneDrive.
- Teams.
- SharePoint.

Please **do not** store any documents on:

- Local drives on your personal device.
- Your own Cloud storage.

Documents stored on your personal device (phone, laptop etc) within the M365 applications are fine.

Please ensure that you do not email yourself documents to your own personal email address.

If you're working on a file by yourself, save it to TEDI-London OneDrive. Use OneDrive if it is a document you own but allow others to view or edit on occasion.

You can use OneDrive to share photos, Microsoft Office documents, other files, and entire folders with people. The files and folders you store in **OneDrive are private until you decide to share them** and you can see who a OneDrive file is shared with or stop sharing at any time.

We use One Drive for business so have the option to restrict the level of access (anyone with the link, only people within your organization, only people with existing access to the file, or only individuals you specify). Also, if you opt to disable editing, you can also opt to prevent viewers from downloading the file.

OneDrive provides a consistent, intuitive files experience across all your devices, including web, mobile, and the desktop of your Windows PC or Mac.

TEAMS

We are using MS Teams for collaboration. Each Team has its own SharePoint site and all members of that Team will have access to those files. Nobody outside the Team will have access unless the permissions are changed in SharePoint. So, by default you can be sure that any files stored within a Team can only be seen by members of that Team.

Use Teams when the file / document is a shared document that the whole team need to access and work on regularly.

Files that you share in a channel are stored in your Team's SharePoint folder. Which can be found in the **Files** tab at the top of each channel.

Any files stored within a private channel in a Team will only be accessible to those members that have access to that private channel.

Files that you share in a private or group chat are stored in your OneDrive for Business folder and are only shared with the people in that conversation. These will be found in the **Files** tab at the top of a chat. It is not recommended to use the chat feature for long term management of documents, please transfer either to a suitable channel in Teams or your own OneDrive. This ensures integrity of the master copy and visibility of the document in the correct place.

SHAREPOINT

SharePoint provides the content services for all files in Microsoft 365, including files you work with in Teams and Outlook.

With both OneDrive and SharePoint, your files are stored in the cloud. You can sync either OneDrive or SharePoint files to your computer. See Sync OneDrive files or sync SharePoint files for more info. The local copies are stored securely within the Microsoft apps.

We do not have any standalone SharePoint sites currently at TEDI-London. It is recommended you store files either within SharePoint site attached to an MS Team or your own OneDrive.

FIVE MUSTS

1. You must only store files and documents within the OneDrive of SharePoint/Teams.
2. You must not store any files or documents on your device outside of the Microsoft applications.
3. You must use OneDrive for files or documents you own, ensuring sharing permissions are set appropriately.

4. You must use Teams for files or documents that are shared and ensure that they are saved in the appropriate channel.
5. You must avoid using Teams chats for long term storage of documents.

ANNEXE 2: TEDI-LONDON PASSWORD GUIDANCE

You may be prompted to change your password on first login. It is good practice to change your password after first logging in. Good password selection protocol can be found here. Your TEDI-London password does not expire, but we recommend that you change it annually or if you suspect that it may have been compromised.

Do	Don't
Do make the new password significantly different from previous passwords.	Don't use the same password for different accounts. Do not reuse your TEDI-London password anywhere else on the web.
Do use a sentence or phrase converted into a string of initials, numbers, and symbols.	Don't use a single word for your password like "password," "monkey," or "sunshine."
Do make your password hard to guess even if someone knows a lot about you (avoid names and birthdays of your family or your favourite band).	Don't use common passwords like "password," "iloveyou," or "12345678."