 [Translated from Spanish to English - www.onlinedoctranslator.com](https://www.onlinedoctranslator.com/en/?utm_source=onlinedoctranslator&utm_medium=docx&utm_campaign=attribution)

**Policyacceptable use**

**1. Introduction**

The purpose of this policy is to provide a broad, general framework for all users of Dō University computers, telephones, and internet services to understand their permitted use. This policy does not cover all circumstances, so all users are reminded to adhere to its general spirit.

**2. Revision history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summaryof changes** |
| 5 |  | Diana Stirbu | Add historyof reviewsAdd reference toJanet's acceptable use policy Add reference to telephone recordings Change references from 'CSU' to 'IT Services' Review clean desk clausesReviewthe essential clauses on cybersecurity |
| 5.1 | November 24th | ElisabethAlmodovar | Add references to KCSIEand PREVENT Duty Add Artificial Intelligence section Add AI meeting assistant text |
| 5.11 | December 24th | ElizabethhAlmodovar | Minor modificationsin information governance |

**3. Scope of this Policy**

3.1 This policy applies to anyone whouse the facilitiesof Technologies of the

 Information (TI) providedbyDō University.This includes our staff, students, membersof the board of directors, contractors, and visitors. Throughout the policy, these individuals will be referred to as "users."

3.2 IT facilities are vital to the operation of lto Dō University.This policy establishes the framework within thewhich ones users can useIT facilities.

3.3 The phrase “IT facilities” encompasses, but is not limited to, computers, software, peripheral devices, issued identitiesby the Dō University, resourcesonline orbased on the cloud, email, phones, Internet access including WiFi, and data stored within computer systems.

3.4 The term "personal data" is defined under the Data Protection Act. In this context, the Group is considered the data controller.

3.5 The Group will request explicit consent from all users that they haveread and understood this policy.One way to obtain this conformity is throughlist of verificationinduction or the declaration form at the end of this policy. Users will also receive periodic reminders that their use of the Group's IT facilities must comply withwith thispolicy.

3.6 This policy should be read in conjunction with:

• Computer security policy

• Data Protection Policy

• Record retention policy

• Staff Code of Conduct

• Janet Acceptable Use Policy (https://community.jisc.ac.uk/

library/acceptable-use-policy)

**4. Distribution**

4.1 This policy, togetherwith all The rest are available on the staff intranet. During their induction, all staff will be informed where to find Group policies, including this one.

4.2 An abbreviated version of this policy is displayed during the login process of the

 computer.

**5. Useacceptable**

5.1 In general:

• IT facilities are provided as resources to support the Group's daily activities,For example, to continuea study program. If you have any doubts about whether the intended use of these resources is relatedwith the business activity, consult firstwith his immediate superior.

• Must not intentionally interferewith the operationfrom the Group's IT facilities, computers, network, or telephone systems; or connect or disconnect any device; or install any software; or attempt to gain access to restricted systems without prior approval from IT Services.

• A user identitycan only be used by the person to whomis granted. This person is responsible for the use and protection of the credentials.

• The softwareshould only be usedOKwith the termsof the license.

• Users must use a unique password that complies withwith the complexity requirementsand updated as described in the National Cyber ​​Security Centre's guidance and IT Security Policy.

• Users should log out or lock their workstation when leaving their computer, tablet, or mobile device unattended to prevent unauthorized access to IT facilities.

• Users should keep their screens clear to prevent unauthorized persons from easily viewing the information displayed or from being captured by nearby cameras or other recording devices. They should also consider the information displayed on the device to prevent personal and confidential information from being shared when sharing their screens through video conferencing software.

• Users should maintain a “clean desk,” ensuring all paperwork and removable media are locked away before leaving the desk unattended.

• Users must complywith all the legal, statutory and contractual obligations that are relevant to their role.

• When leaving the Group, users must inform their line manager before departure about any important information contained in their account and, if necessary,be like this, make surethat your line superior has access to it before your departure.

5.2 The data protection requirements are:

• All the staff must complywith the policyGroup Data Protection in the handling of personal data.

• The creation of student data sets outside of the Group Management Information System mustbe approved previouslyby the director ofInformation andFinancing.You may be required to complete a Data Protection Impact Assessment before obtaining approval.

• Users should not store personal data on mobile devices (tablets, smartphones, smartwatches, etc.).), devices portable storage (USB flash drives, hard drives

removable,etc.) or in cloud storage services not providedby the Group (Dropbox, OneDrive,etc.) without an approved risk assessmentby the director Information Technology. This risk assessment may take the form of an Impact Assessment

of Data Privacy.

• Users must take precautions to protect all computer media and mobile devices when taking them outside the Group's premises (For example, avoid leaving a laptop unattendedor displayed in a car in a manner that could encourage opportunistic theft).

• Users should not use their work email address to subscribe to newsletters.by mail electronicor register for social media accounts without a clear commercial use that would allow them to do so.

• All exchange of classified data, including personal data,with organismsexternal must be carried outSecure data sharing methods include encryption, direct transfer, and the use of trusted third parties. Such data sharing must also comply with permitted usage.by the policyand the Group's data protection notices, or authorization will be requested from the persons involved.

• Sending personal data via WhatsApp or other unauthorized social media messengers is not permitted.

• The sending of personal data is not permitted.by faxFax is considered unsafe and,so so much,It is not suitable for sending or receiving information from classification higher thanthe public one.

5.3 The privacy requirements are:

• Access to a staff member's email and file storage may be granted to the immediate superior or another staff member delegated by the superior. Such requests must be submittedin writing to thedirector Information Technologyon the part of the immediate superior and accessonly know will be granted when there is a clear business justification.

• User's email and file storage, as well as information provided, may be accessed to comply withwith the legal requirements.This includes

the Group's obligations under data protection and freedom of information legislation.

• Given thatThird parties may be granted access to file storage and email without the user's consent. Users should not assume that their file storage or email is private. Confidential personal matters should not be stored or transmitted on Group IT premises.

• The Group monitors the use oftheir systems computer scientistsand telephone calls to maintain efficiency and prevent misuse. Monitoring is also conducted to identify and escalate protection concerns and to complywith the sectoral and legal requirements, includingChild Protection in Education and the obligation to PREVENT.

• The Group may monitor telephone calls to ensure satisfactory customer service. If a call is monitored, all parties involved will be notified.

• Incoming calls to the Group's landlines are recorded until the switchboard forwards them to a new extension.This treatment is described in anotice of privacyin itplacewebsite of the Clusterand in an automatic message at the start of the call.

• Users must protect classified information they send, receive, store or process.themselves, according tothe assigned classification level, including electronic and paper copies.All material which they believe should be properly labeled.

• Users mustbe aware of your work environment to ensure that they are notpastby highneither heardby people unauthorized when working and must take due care when workingwith information classified.

5.4 The email requirements are:

• A 'disclaimer' or 'foot of page'from group to all outgoing emails.

• Allthe conversationsby mail electronicwith third parties should be considered written on letterheadof the Group and appropriate standards of etiquette and formality must be adopted. Emails should be written following email best practices.

Label.The British Library's guide is an example of good email etiquette practices.

• Users should ensure they have correctly entered the recipient's email address(es) before sending the message, to prevent the breach of classified information. If the email address should not be disclosed, it should be placed in the blind carbon copy (BCC) field.

• Users should not representtheir own pointsofseen as those of theUniversity

 Do nor imply the formation of a contract between the Group and a third party.

• You must not intentionally send, receive or forward material that may be considered obscene,illegal or defamatoryor that is intended to annoy, harass or intimidate another person.

• All the email will be automatically scanned to identifyviruses and bulk mailUnwanted (also known as spam). No email from addresses listed in theblacklist.

• Email mailbox sizes will be limited, and outdated files will be deleted without prior notice. Retention periods apply to the Group's email system. Please refer to the record retention policy for the retention periods applicable to each mailbox folder.

5.5 The Internet requirements are:

• The Group will record and filter Internet usageon the part of our users in accordance with our sector and legal requirements, including those for keeping children safe in education and the duty to PREVENT.

• Unauthorized use of instant messaging or peer-to-peer file sharing software is not permitted.

• Users must not upload or download materials thatviolate the rightsof author.

• Users must not access or distribute material that does not represent the group's core values. This includes material that could be considered obscene,illegal, defamatory or that may harass or intimidate others.

5.6 Use of personal devices:

• The use of personal devices to access Group systems is at the owner's own risk and the Group accepts no liability.

• Storing personal data of the Holding Group on personal devices is discouraged, and appropriate security measures must be implemented to ensure its protection against unauthorized disclosure. A device is considered to have adequate security measures if it meets the following requirements:with everyone the criteria of the current cybersecurity specification, available at thewebsite.

• The registration of a personal device in a Group service where the personal data relatedwith the Group can be transferredthe device implies acceptance that the Group may:

- Deletedata remotely in case the person leaves their employment with the Group or the device is lost.

− Enforce a minimum level of security remotely (For example, encrypted,

 access with PIN, screen lock).

- Requirethe installation of additional software on the device to support secure use of the service (such as Microsoft Authenticator to support multi-factor authentication).

5.7 Use of Artificial Intelligence tools

• AI tools should not be used to falsify human likenesses without express consent. This includes, but is not limited to, text, images, and videos.

• Use of meeting assistantswith AI

Meeting attendeeswith AI They usually storetranscripts and other meeting data, such as videos or email addresses, in unauthorized locations and under various complex privacy agreements. These maybe invited tothe meetingby othersparticipants, sometimes automatically.The meeting organizer should ensure that any unrecognized external participants are questioned.

If you are using an AI tool for meeting transcription, then you should

Inform tomeeting participants and obtain their consent before joining the meeting tool.

The only tool approved for Microsoft Teams is the built-in transcription feature. If you need more features, seewith the Governance Teamof the Information to use another product.

5.8 The primary purpose of providing computer, network, or telephone systems is to support the Group's activities. Limited personal use is permitted under the terms of this policy and the following:

• The primary purpose of the service should always be given priority.

• Personal use should not interferewith the correct operationof the service.

• Personal use of the Internetonly performs outsideof the working day (or during breaks) and must not affect the performance of the user's duties.

• Personal use must not be relatedwith the operationof a company or enter into conflictwith the responsibilitiesof a staff member as an employee of the Group.

• The Group reserves the right to recover costs for excessive personal use.

**6. Consequences of misuse**

6.1 Failure to comply with this policy may result in disciplinary action. Access to computer and telephone facilities may be withdrawn pending the outcome of an investigation or disciplinary action.

6.2 It is the Group's legal responsibility to refer to thePolice the download, view or storeof certain materials (For example, illegal imagesjuvenile).

6.3 If a user detects, suspects or witnesses an incident that may constitute a security breach or observes any suspicion of information security weakness in the systems or services, they must immediately report it to thedelegate Data Protection.

**7. Status of this Policy**

7.1 This policy has been developed applying the best practices of the ISO 27001 standard and is part of the Group's commitmentwith the obtainingand the maintenance of certifications

7.2

cybersecurity.Hedirector Group Operations will periodically monitor its implementation.

Technologiesof the information.

|  |  |
| --- | --- |
| Policy Review Area | HE |
| Senior Manager/Ownerof politics | DirectorInformation Technology Group |
| Approval level | Equipmentgroup leadership |
| Dateof approval | March of 2025 |
| Review cycle | Every two years |
| Next review | March of 2027 |

**Statementacceptable use policy**

Any userof the Group's IT facilities who have not signed an employment contractwith the Group mustread and acceptthe Acceptable Use Policy, sign the following statement and return this page to Human Resources before you can be asked to log in.any PC.

This signed statement must be provided to IT Services along withwith the applicationlogin PC sent to IT Services Help Desk.

**Statement**

I confirm thatI haveread and understoodthe Acceptable Use Policy and that I must comply with it at all times.

I am aware that any breach of this policy may result in withdrawal of IT access and further action.

Name:

Signed:

Date: