Brunel University London

Information Services

IT Acceptable Usage Policy

Contents

1. Document Control

Title	IT Acceptable Usage
Version	1.0
Review by	September 2025
Policy live date	September 2024
Policy owner	Chief Digital Information Officer
Stakeholders consulted in development	IS SLT & Managers Jeremy Baxter – CDEPS Stephen Middlehurst – CBASS Neil Newland - CHMLS Lorna Goodey – Data Privacy Terry Vass – Campus Security Ash Patel – Finance Mark Brown – Procurement Luisa Costa – Legal Team
For information & action	All employees, students and other authorised users of BUL systems
Supersedes	BU-POL – AUP BUL-POL-EMAIL BUL-POL-6.2.1 – Remote Working BUL-POL-Social Media Use
Supporting policies	**Under review/to be drafted** Information Security Policy Information Security Awareness Policy Identity & Access Management Policy Password Management Policy Bring Your Own Device (BYOD) Policy Security Incident Management Policy Supplier Security Management Policy

2. Purpose and Background

2.1 The IT Acceptable Usage Policy (ITAUP) aims to provide clarity on the behaviours expected and required by BUL employees, students, alumni and other authorised users, in order to protect the individual and BUL.

2.2 Information technology systems are provided to enable authorised users to contribute to achieving the vision and mission of BUL; intended to promote effective communication and working practices within our organisation, and in the interest of supporting the delivery of learning, teaching, innovation and research to the highest possible standards.

2.3 The following BUL policies and frameworks should be referenced in conjunction with this Policy:

- Information Security Policy
- Data Protection and Information Access Policy
- Records Management Policy & retention schedules
- Safeguarding Policy
- Procurement Policy
- Anti-Bribery and Corruption Policy
- Prevent Policy
- Social Media Use Policy
- International Remote Working Policy

3. Scope

3.1 This Policy outlines the standards we require BUL employees, students, alumni and other authorised users to observe while using information and information systems provided by or through BUL. This includes but is not limited to email, internet, network, voice and mobile IT equipment, software and IT systems.

3.2 This Policy applies whether using your own device or a BUL owned device to access or process information on BUL information systems.

3.3 This Policy applies at all times, both on and off the BUL campus when using BUL information systems and not just during your normal working hours.

3.4 This Policy is taken to include the JISC Acceptable Use Policy, JANET Acceptable Use Policy, Eduroam Use Policy and the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement. The University also has a statutory duty, under Section 26 of 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.

4. Definitions

Account Audit Logs	Account audit logs capture information account which users are performing actions and when.
Alumni	Former students of BUL.
Authorised Users	Contractors, consultants, temporary workers, 3rd parties who have been granted access to BUL's information systems.
Availability	Information and systems available when needed.
BUL Systems Account	Main account used to access BUL email, network services and cloud applications.
Cloud Applications	Software delivered to users over the Internet.
Confidential Data	Information that is confidential to BUL and is not intended for public dissemination.
Confidentiality	Only permitting authorised access to information, while protecting from improper disclosure.
Cyber Security Incident	A breach or attempted breach of an information system in order to affect its integrity or availability.
Data Owner	A senior-level individual or the designated department within BUL that holds ultimate accountability for a specific dataset or data domain.
Data Subject	The identified or identifiable living individual to who personal data relates.
Employees	Fixed term and permanent employees on BUL's payroll.
Information	All information and data held on BUL's applications and systems.
Information Security Breach	Any incident that results in unauthorised access to BUL's data, applications, networks or devices.
Information Security Management System (ISMS)	A framework of policies and controls that manage security and risks systematically across the entire organisation. Typically aligning with a common security standard e.g. ISO 27001
Information Services Team	The Information Services Team at Brunel encompassing the Information Services Directorate and College IT Teams.
Information Systems	BUL's systems, devices, services (e.g. Internet, email, "bring your own device" (when connected to the University systems) and telephony, applications and information in logical and physical form as well as any other University equipment. This also includes service providers' systems/equipment when provided to BUL.
Integrity	Information is recorded, used and maintained in a way that ensures its completeness, accuracy, consistency and usefulness for the stated activity.
May/Should	Refers to items regarded by BUL as minimum good practice, but for which there is no specific legal requirement.

Network Device	A physical or virtual component used to facilitate communication and data transfer within a computer network. E.g. routers, switches, firewalls
Personal Data	Information relating to a Data Subject, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) or an opinion about that person's actions or behaviour. It does not include anonymised data.
Privileged Access Account	System access account that provides elevated access to administer a system and/or view restricted data.
Remote Access	Any access to BUL's network through a non-BUL controlled network.
Single Sign-on	Authentication method that enables users to securely authenticate with multiple applications and websites using one set of account credentials.
Students	All individuals participating in a course of study at BUL (undergraduates, postgraduate research, executive students)
User endpoint device	Laptops, notebook computer, desktop, tablet
We	Brunel University London (BUL)
Will/Shall/Must	Equals 'is required to'. It is used to indicate mandatory requirements to be strictly followed to conform to the standard and from which no deviation is permitted.

5. Policy Statement

5.1 Key Principles

Acceptable use is that which is lawful and in accordance with BUL's objectives and policies. The security of BUL's data network against unauthorised use and access must be a primary concern of each and every user at all times.

Individuals will be granted access to BUL's information systems on their justifiable operational need.

It is a clear breach of this Policy to act with disregard - whether wilful or negligent - of best information security best practice, and such disregard may be dealt with under BUL's disciplinary procedures.

The absence of a prohibition within this Policy shall not be taken to mean that permission is granted. Advice must always be sought from BUL Information Services Team.

5.2 Policy Framework

This Policy is part of BUL's Information Security Management System, and should be read in conjunction with the BUL Information Security Policy, BUL Data Protection & Information Access Policy and any other relevant policy as mentioned in this document.

5.3 Accountability

Brunel's Chief Digital Information Officer (CDIO) has overall accountability for this policy.

The CDIO will be accountable for implementing and enforcing this Policy and ensuring that all employees, students and other authorised users receive guidance on IT acceptable usage.

5.4 Key roles & responsibilities

Head of Cyber Resilience

The Head of Cyber Resilience is responsible for the production, maintenance and communication of this Policy and has overall responsibility for maintaining and ensuring compliance against this Policy.

BUL Information Services Team

BUL Information Services Team will implement technical controls and procedures to enforce this Policy.

It is the Information Services Team's responsibility to ensure that:

- the technology estate (user devices, infrastructure, networks, applications & systems) is secure and compliant to all relevant Acts and laws.
- actual cyber security incidents are reported via BUL cyber security incident management process.

BUL Line Managers

Line managers are responsible for ensuring that their team – including contractors, temporary staff and any third parties – are aware of and understand:

- This Policy and all supporting policies and procedures applicable in their work areas.
- Their personal responsibility for information security.
- How to access advice on information security matters.

In addition, Line managers are responsible for:

- Ensuring that their team have completed all mandatory compliance training on information security awareness, relevant to their role.
- The acceptable use of information and information technology within their team.
- Ensuring that no new software system or tooling is procured in their area of responsibility without appropriate due diligence and involvement of Information Systems, Data Protection and Legal Teams.
- Ensuring that system accounts are disabled, and equipment and data is recovered from leavers – including employees, contractors, temporary workers and third parties.

Employees, Students and other Authorised Users

All employees, students and other authorised users must ensure that they have read and understood BUL's Information Security Policy and supporting policies, as well as completed all mandatory training on information security awareness, relevant to their role.

All employees, students and other authorised users must always comply with this Policy to protect BUL's electronic communication systems, data and equipment from unauthorised access and physical damage.

All employees, students and other authorised users are responsible for:

- The security of BUL's IT equipment and data. IT equipment must not be left unattended other than at home or within secure office spaces on campus, with equipment either locked or logged off to prevent unauthorised access.
- Ensuring that all sensitive/confidential information is removed from workspaces and meeting rooms when not in use.
- Ensuring that non BUL equipment used to access BUL's IT resources are maintained, updated, and comply with the requirements set out within BUL's Bring Your Own Device (BYOD) Policy.
- Ensuring that all BUL IT equipment and data are returned on termination of their employment contract or on leaving the University.
- Reporting actual, suspected and potential cyber security incidents to the IT Service Desk as soon as they are aware of them and assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.
- Ensuring that the necessary due diligence is completed before introducing new technology products in accordance with BUL's Supplier Security Management Policy.

5.5 Exemptions

Where it is not possible to apply or enforce any part of this policy (for example, legitimate research, teaching and academic activities that could be considered unacceptable use), then a request must be raised with the IT Service Desk in the first instance. BUL's Head of Cyber Resilience will review the business justification and advise on the associated risks. Policy exceptions will only be issued when the relevant Data Owner has signed off on the identified risks.

This policy may have an impact on users of assistive technology or assistive software due to their disability. These individual cases will be considered on a case by case basis.

Any potential research involving obscene or indecent material must always be approved by BUL's Legal Team.

5.6 Policy Compliance

Compliance with this Policy and all supporting policies and procedures is a requirement for all employees, students and other authorised users.

BUL reserves the right to monitor system use, including analysis of account audit logs. Any such examination or monitoring will only be carried out by authorised and trained individuals.

Technical security controls and processes will be implemented by BUL's Information Services Team to support the required procedures and settings for BUL system use.

Non-Compliance

Any evidence of non-compliance with any aspect of this Policy or any supporting policy or procedure should be raised with the CDIO via the appropriate University authority (such as Director of HR, Head of Privacy, Head of Security and Campus Support Services).

The CDIO, or designated agent, has the authority to:

- Withdraw access to all or any subset of information systems, or to commute such sanction by issuing a warning of unacceptable use.
- Restrict or terminate a User's right to use the BUL network.
- Withdraw or remove any material uploaded in contravention of this Policy.
- Where appropriate, disclose information to law enforcement agencies.

Breach of this Policy and any supporting policy or procedure may be dealt with under BUL's disciplinary procedures and, in serious cases, may be treated as gross misconduct. Legal action may be taken by BUL in any instance wherein it is deemed to be in the interests of the University to do so.

Any risks arising from non-compliance must be recorded on the relevant risk register and proportionate mitigation action put in place.

5.7 Policy Review and Maintenance

This Policy and all supporting policies and procedures that form BUL's Information Security Management System (ISMS) will be reviewed and updated on an annual basis to ensure that they:

- Remain operationally fit for purpose;
- Reflect current technologies;
- Are aligned to industry best practice; and
- Support continued regulatory, contractual and legal compliance.

6 BUL System Use

6.1 Access credentials are issued for the sole use of an individual; these will include, but are not necessarily limited to, a username and password.

6.2 Multi factor authentication (MFA) must be in place for all cloud application accounts. MFA verification should be via a BUL approved MFA Authenticator App and in accordance with BUL's Identity and Access Management Policy

6.3 Generic or group IDs shall not normally be permitted as a means of access to BUL's information systems but may be granted under exceptional circumstances where sufficient access controls are in place to protect the account.

6.4 Generic identities must never be used to access confidential data or personally identifiable information.

6.5 Privileged access accounts for system administration must only be accessed via a BUL owned device.

6.6 BUL systems accounts must be logged into at least every 180 days, failure to do so may result in the account being locked.

6.7 Employees, Students and other authorised users must ensure that they have read and understood BUL's Password Policy. All passwords must be set in accordance with this policy.

6.8 Individuals must take all possible precautions to protect their access credentials and never share them with anyone at any time.

6.9 Individuals must never grant access to BUL information systems with anyone at any time, unless authorised to do so as part of their role.

6.10 No individual shall masquerade as another using login names and passwords, which are designated for individual use.

6.11 Individuals who believe their credentials may have been compromised must immediately change their password and report it to the IT Service Desk for further investigation.

6.12 Individuals must not attempt to gain access to restricted areas of BUL's systems, which is not required for their role, unless specifically authorised in accordance with BUL's Identity & Access Management Policy.

6.13 The use of BUL's information systems is prohibited when the use is deemed unacceptable. Unacceptable use includes, but is not limited to:

- Any activity regarded as unlawful or potentially unlawful.
- Disclosing personal identifiable information and restricted or confidential information to unauthorised individuals.
- Compromising passwords (e.g., by using weak passwords, reusing them, making them visible to or disclosing them to others)
- Creation, download, storage, transmission or display of:
    - Any offensive, obscene, or indecent images, data or other material or any capable of being resolved into obscene or indecent images or unsolicited material.
    - Material with the intent to cause annoyance, inconvenience or anxiety.
    - Material with the intent to defraud.
    - Material that promotes or discriminates against anyone because of age, gender assignment, being married or in a civil partnership, being pregnant or on maternity leave, disability, race including colour, nationality, ethnic or national origin, religion or belief, sex.
    - Material that incites racial or religious hatred, terrorist activities, or hate crime, or instructional information about any illegal activities
    - Defamatory material (e.g., cyber bullying)
    - Material that could damage BUL's image or reputation
    - Material such that this infringes the copyright of another person
- Unsolicited bulk or marketing material unless using BUL's email marketing tools, and in accordance with the Privacy and Electronic Communications Regulation (2003), see Data Protection and Information Access Policy.
- The use of BUL's information systems for any commercial or business activity that is not in accordance with the aims and policies of BUL.
- Deliberate unauthorised access to BUL equipment, facilities, or property.

- Storing material downloaded for personal purposes on BUL systems.
- Corrupting or destroying other individuals' data.
- Violating the privacy of other individuals.
- Continuing to use an item of technology after the Information Services Team has requested that use ceases as it poses a potential risk to the University.
- Knowingly or recklessly introducing harmful software (e.g., malware) or opening attachments from unknown or untrusted sources.
- Disabling security or email scanning software.
- Signing up to 'free' or 'trial' versions of any software via their BUL account, as it generally allows for data/content to be used by the company, which may have implications not just for personal data, but for the University's business data and intellectual property rights.
- Connection of any internet enabling device or other external link, enabling remote access to any BUL system without permission. For example, unauthorised VPN software.

6.14 Any information stored on or shared via BUL's systems is subject to data protection and law enforcement legislation and should be managed in accordance with BUL's retention and disposal schedules.

6.15 BUL reserves the right to use monitoring activities to protect against threats to the university community and to the University itself.

6.16 In certain circumstance it may be necessary for a member of the Information Services Team to access an individuals' BUL systems account, for example to investigate a technical issue, to grant access to another individual for business continuity in their absence, or in other exceptional circumstances. Requests for access must be raised with the IT Service Desk in the first instance, with either agreement from the individual for Information Services or another individual to access their account, or if the user is unavailable, in consultation with a member of the HR and Privacy Teams.

6.17 BUL reserves the right to withdraw access privileges and report to the appropriate authority any user who uses the internet for illegal purposes.

7. Email Use

7.1 Authorisation for a BUL email account will either be triggered by the HR system for employees, and the Student Records system for students, except for contractors and third parties where delegated processes are in place.

7.2 An official BUL email account must be used for all communications on behalf of the University to ensure traceability and security of BUL data and information.

7.3 BUL email accounts should not be used to sign-up to services used outside of the University. E.g. shopping sites, social media

7.4 Email containing University Confidential information must be encrypted when sending to external recipients outside of the organisation.

7.5 Email communication with under 18s must comply with the BUL Safeguarding Policy.

7.6 In situations where a shared mailbox is required, access to it will be configured through an individual's BUL account.

7.7 Shared mailbox sponsors are responsible for ensuring that appropriate access is maintained.

7.8 Automatic forwarding of emails from a University owned email account to an external email account is not permitted.

7.9 Legacy email protocols (POP, IMAP, Remote PowerShell, Exchange Web Services (EWS), Offline Address Book (OAB), Outlook for Windows, and Mac) are not permitted to connect to BUL email systems.

7.10 Native mail apps (e.g., Apple's iPhone Mail app, or the Gmail app on Android) are not permitted to access BUL email.

7.11 File attachments larger than 35MB are not permitted to be sent or received by BUL email accounts.

7.12 Certain file extensions are not permitted to be sent or received, click here for more info.

8. BUL Networks

8.1 Individuals must not attempt to gain access to restricted areas of the network, or to any password-protected information, which is not required for their role, unless specifically authorised in accordance with BUL's Identity & Access Management Policy.

8.2 Only authorised individuals may physically access the BUL data centres, communications (comms) room or IT cabinets.

8.3 Smoking, eating and drinking is strictly forbidden in areas housing network equipment or servers.

8.4 Only authorised BUL devices shall be allowed to connect to the BUL wired or wireless network. All other devices and personal devices must never be physically connected to the BUL staff network. However, they are permitted to connect to the Guest Wi-Fi network or Eduroam.

8.5 In highly critical infrastructure areas (data centres, comms rooms) individuals must not add or remove, modify, connect to or disconnect from the BUL network any equipment unless approved in writing by the Head of Infrastructure Operations and supported by an IT Change Request.

8.6 Individuals must not connect a wireless access point to the BUL network unless approved in writing by the Head of Infrastructure Operations and supported by an IT Change Request

8.7 No individual shall download/share large files or stream online services that could impact BUL network performance.

9. Privileged Access

9.1 Privileged access means access to BUL systems and data that has been granted to an individual beyond that of a typical user. For example, administrative access to a system, access to sensitive personal data on a HR system.

9.2 Privileged access must be via an individual account with a unique username and password, which is separate from their day-to-day user account.

9.3 Privileged access accounts must not be used for high risk or day to day user activities, for example web browsing and email.

9.4 Privileged access accounts must only be used to perform authorised duties where responsibility is part of the individual's assigned role duties.

9.5 Individuals with privileged access rights are required to sign agreements annually to reinforce the Information Security Policy and ensure ongoing compliance.

9.6 Individuals with privileged access shall take all necessary precautions to protect the confidentiality of information encountered in the performance of their duties, and data must not be used for purposes other than those already authorised.

9.7 If methods other than using privileged access will accomplish an action, those other methods should be used unless the burden of time or other resources required clearly justifies using privileged access.

10. User Endpoint Devices

10.1 BUL purchased user endpoint devices (e.g. laptops, notebook computers, desktops, tablets) must be procured and configured by the Information Services Team.

10.2 Equipment procured by BUL is owned by BUL and the individual in receipt of the equipment is accountable and responsible for its use and storage until it is formally returned:

- Must protect their BUL device from loss, theft and damage, and must also report any loss or theft to the IT Service Desk within 24hrs.
- Must not allow their BUL device to be used by unauthorised users.
- Must not attempt to deactivate, bypass, tamper with or reconfigure any protection installed on the device e.g. antivirus service, desktop firewall, services to install security patches or any other security measures that BUL has in place.
- Must not install, un-install or change the configuration of software on their BUL device. All software must be approved and installed by the Information Services Team.
- Must only use software (including cloud applications) that is authorised by BUL on their BUL device. Authorised software must be used in accordance with the software supplier's licensing agreements.
- Must not store local copies of confidential or personally identifiable information on their BUL device. This information must be held securely within approved BUL systems and or storage areas.

- Must cease to use their device if they believe it has become infected with malware and immediately report to the IT Service Desk for investigation.

10.3 Users should take all reasonable steps to report any faulty equipment to the IT Service Desk, and endeavour to leave computers in a clean, usable state.

10.4 Line managers are responsible for ensuring that all equipment and data is recovered from their direct reports on termination of their employment contract or on leaving the University.

10.5 Individuals using non BUL equipment (computers, laptops, smart phones and/or tablets) to access and use BUL IT resources, must comply with BUL's Bring Your Own Device (BYOD) Policy.

11. Printing

11.1 If there is a requirement to print documents containing personal or confidential information this should be carried out on a BUL multi-function printer, requiring user authentication to release the print job.

11.2 All paperwork printed that holds personal or confidential information must be held in a locked drawer or filing cabinet and destroyed via BUL's confidential waste disposal service.

12. Working Remotely

12.1 Employees, Students and other authorised users must always be conscious of the physical environment when working remotely, ensuring no one is looking over their shoulder at information on their device.

12.2 Unprotected public WiFi networks (e.g. no password required to access) must not be used for carrying out BUL work.

12.3 When working away from the campus or your home network, it is advisable to use mobile tethering as an alternative to public Wi-Fi, but BUL cannot be held liable for the use of a personal mobile phone including any data charges, and so any use of a personal phone for this purpose is the individual's choice.

12.4 If it is necessary to use public WiFi the hotspot must be secured by the provider (e.g., train, conference venue, hotel, coffee shop) with a password to grant access and a clearly named network to connect to from the list of available WiFi networks. Employees, Students and other authorised users are responsible for checking the providers Ts & Cs before connecting to the network to carry out their BUL work.

12.5 VPN access to information systems hosted on the BUL network is only permitted via a BUL approved VPN client.

12.6 It is the responsibility of individuals with VPN privileges to ensure that these privileges are protected and not shared with unauthorised users.

13. International Working

13.1 The Information Services Team must approve the use of BUL issued equipment abroad and this must be supported by an International Remote Working Request Form in accordance with BUL's International Remote Working Policy.

13.2 Employees, students and other authorised users accessing BUL information systems from other countries must be familiar with what measures they can take to limit the potential for threats to expose vulnerabilities and create risk.

13.2 Where there is a requirement to access BUL information systems from countries considered as high risk, this must be discussed with the Information Services Team and appropriately risk assessed.

14. Social Media

14.1 The use of social media for BUL purposes shall be in accordance with BUL's Social Media Use Policy.

14.2 Employees, students and other authorised users must not use their BUL email address on their private social media accounts as this may compromise the security and privacy of BUL's email system.

14.3 In line with data protection principals, personal social media channels must not be used for sharing sensitive and/or confidential/personal information.

14.4 BUL M365 (Email, Teams, Viva Engage) and Intranets are the approved communication tools and must be used for all BUL related internal communications.

14.5 Public social media may only be used for BUL purposes by using official BUL social media accounts with authorisation from the External Communications Team. Users of official BUL social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

14.6 Official BUL social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts in accordance with the BUL Password Policy.

14.7 Users shall behave responsibly while using any social media whether for BUL or personal use, bearing in mind that they directly or indirectly represent the University.

15. Classification – University Confidential & Personal Data

15.1 Users must ensure that all University information (including third party information held by BUL) is classified correctly and treated appropriately in accordance with BUL's Information Classification Policy and retention schedules.

15.2 Everyone working with or using personal data that is not their own has a responsibility to ensure appropriate confidentiality is maintained, and in accordance with the BUL Data Protection and Information Access Policy.

15.3 All employees, students and other authorised users are responsible for ensuring that appropriate access to data is maintained in accordance with the BUL Data Protection and Information Access Policy and any other contractual obligation from data providers they must meet.

15.4 University confidential and/or personal data must not be stored on removable electronic media or locally on any device. Any data downloaded must be deleted from the device immediately after accessing.

15.5 Copies of University confidential and/or personal data must not be taken stored/saved to any location that is not within BUL approved systems and/or storage areas.

16. Payment Card Data

16.1 Only individuals who have been allocated with and trained to use card payment devices are permitted to use them.

16.2 A central register will be maintained of all payment card devices owned or leased by BUL, with all devices inspected on a regular basis.

16.3 Users shall never store payment card data for any reason without approval from BUL's Finance Department. This includes printing it or writing it down on paper.

16.4 Guidelines for storing and protecting payment card data must be compliant with PCI data security standards.

16.5 An annual review will be conducted of BUL's payment card environment and controls to ensure PCI-DSS compliance.

17. Introducing new technology

17.1 The introduction of new technology must meet BUL's minimum technology and security requirements and be in accordance with BUL's Supplier Security Management Policy.

17.2 Individuals responsible for agreeing supplier contracts on behalf of BUL are responsible for:

- ensuring that adequate background screening is conducted, in accordance with BUL's Procurement Policy.
- ensuring that the necessary security due diligence is completed before entering into a relationship with a supplier, including an information security and data protection impact assessment.
- ensuring that any variations to BUL's standard terms and conditions comply with BUL's Information Security Policy and are authorised by the Procurement Team, who will seek advice on alternative clauses from Legal Services as appropriate.

- assessing if restricted/confidential information will be shared with a supplier, and consulting with the Legal Team for guidance on non-disclosure agreements.
- ensuring that requests to share University information beyond the supplier have been signed off by Data Protection and Privacy Team.
- ensuring that supplier renewals include a review of the supplier's information security controls

18. Security Incident Management

18.1 Actual, suspected, threatened and potential cyber security incidents must be reported in a timely manner to the IT Service Desk.

18.2 Incidents that involve personal data must also be reported to BUL's Data Protection Officer.

18.3 Employees, Students and other authorised users are responsible for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.