JLC
IT SERVICES

IT Policy

Revision 9 (June 2024)
IT Manager

JLC
JOHN LEGGOTT
COLLEGE
inspiring education
EST. 1968

Introduction

This policy explains the key aspects of IT Use & Security across John Leggott College. The policy is applicable to all staff, students and external users of college IT systems and services. Any violations of the policy could be subject to the staff and/or student disciplinary policy.

Staff are responsible for reading and implementing all John Leggott College policies.

This policy is owned by the IT Manager and is updated annually.

This policy is split into the following sections;

- Students - IT Use
- Staff - IT Use
- Services
- Infrastructure
- Security

Key Definitions

JLCNET – The JLC computer domain.

Microsoft Office 365 – the system used for college email,

Google Apps Suite – the Google Apps suite of products used by staff and students for questionnaires, Google Classroom resources, document storage and collaboration.

IT Helpdesk – the physical IT helpdesk which is located in the Portal.

IT Service Portal – the online IT service system used for logging problem tickets and getting useful information and guides on using JLCNET and related services.

PaperCut – our managed print system used for printing and copying in college.

Related Documents

This policy is to be read in conjunction with other college policies. e.g. Disciplinary Policy and the Code of Conduct.

The following policies and procedures are included in the IT Use Policy;

- IT Security Policy
- IT Management Procedures
- Data Protection Policy
- eSafety Policy
- Cyber Security

JLC
IT SERVICES

Students

Students studying at John Leggott College are issued with a unique username and password which allows access to the main JLCNET network and related services.

The username and password will be issued during the transition period.

The username will be a student's student number.

A generic password will be issued for students to change at first logon when they start with us in September. Upon starting at college, students should reset their password and choose a password that is as complex as possible. Once students start at JLC, they will be required to set up MFA (multi-factor authentication) to be able to access resources outside of the John Leggott College network.

A Standard Student Account

Standard student user accounts are provided with a private documents area (Drive H:) and a public shared student area for accessing some curriculum materials.

Selected teaching staff have access to student document areas for the purpose of work retrieval.

Student accounts are provided during the transition period. The accounts provided during these days will allow students to see the JLCNET environment and access CEDAR. Further enhanced functionality such as email, printing and guest WiFi access will not be enabled until the student starts college in September.

Staff

Staff working at John Leggott College are issued with a unique username and password which allows access to the main JLCNET network and related services.

The username and password will be issued following a ticket logged by HR, the account will allow them access to Google Classrooms for the purpose of completing the staff induction. Once the staff induction has been completed, following a second ticket logged by HR, IT Services will modify the account to have access to all features (email, G Suite, JLCNET, AllStaff email, etc.).

The username will be their full name with no spaces. In the event that this is in use, an increasing number will be appended (1, 2, 3, etc.).

A unique password will be issued for staff to change at first logon. Staff are required to change this password at first logon. Staff should choose a password that is as complex as possible. When staff start at JLC they will be required to set up MFA (multi-factor authentication) to be able to access resources outside of the John Leggott College network.

Where data is stored within the confines of a user's account, it might be necessary to reset the user's password in order to gain access to support the functions of the college. In this case, the user's new password will be conveyed to them in as sensitive a manner as possible. Before granting access to a user's account to another college employee approval will be sought from HR.

A Standard Staff Account

The ownership of data held on the JLCNET system lies with John Leggott College. If an individual leaves employment with John Leggott College, sufficient arrangements must be made to transfer any data to either a head of subject, area or central HR personnel. Data required by others on a day to day basis must be stored in a shared area. Either on the network shared area, or Google Drive shared folder. Upon leaving staff must obtain prior consent before transferring any data off the John Leggott College network.

Staff should be aware of the data they have access to. Data access on the JLCNET system is provided by roles. Each staff member will be part of one or more roles and their roles define the data they have access to. Please see the IT Security Policy for more information. If staff members notice they have access to more data than they should, they must report this to IT Services immediately.

How Users can get help with IT

There are three main ways for users to get help with IT issues. Users can call in to the student helpdesk in the portal where a ticket can be logged on the iPad for immediate support. Users can also log a ticket by emailing IThelpdesk@leggott.ac.uk, or by visiting the ticket logging system available from any new tab page on a PC. Staff are also able to call IT Services using 8x8 and dialling 1000.

How IT Services publish information

IT Services distribute information through leaflets available across from the IT Helpdesk, through slides available in tutorials and send information out via email to Staff and Students.

JLC
IT SERVICES

What to use for what

There are a range of IT systems that are used for specific things. Here's a list of the common things we use at John Leggott College.

- IT Service Dashboard – providing links to all commonly used systems.
- PaperCut – the college wide printing system.
- Microsoft Office 365 – a system used for email.
- Google Apps – a document collaboration and storage system used by subject areas for teaching & learning resources, online meetings, document storage, and other Google Services as they become available. Google Apps is NOT used for email (Gmail is disabled).

PaperCut

The college uses PaperCut as its managed print system. Users can print to the JLC-FollowMe printer and go to any print device to collect their document. The system works on a credit basis. Printing charges can be obtained by emailing printandcopy@leggott.ac.uk, or logging a ticket with the Print and Copy helpdesk.

Users should monitor their print use using the PaperCut system installed on all college machines.
If students run out of print credits they can top up their balance at Student Reception located in the main entrance to college. Staff printing is recharged to departments based on the selected shared account.

Printing jobs, wherever possible and practical, should be directed to the reprographics department. Large jobs (jobs over 100 pages) should be sent to reprographics for printing.

Guest Networks

The college operates a Guest access wireless network (JLC User Devices). Users have access to the guest network for internet access on their personal devices. Internet activity via the guest network is logged and monitored in the same way as a connected college owned device.

Students are required to pay the campus charge to maintain access to the guest network. The campus charge also includes other services such as inclusive printer credits. Please check with Student Services for a full list of what is included in the campus charge.

Users must ensure that their devices connected to the guest network have the latest operating system updates and sufficient Anti-Virus software is installed and up to date. Devices that do not run current Microsoft supported versions of Windows, Apple supported MacOS, iOS, Android or other operations systems will not be supported on the network in case of access issues.

The IT Services staff reserve the right to disable a personal device from the guest network if that device is deemed to be a security risk, is using too much bandwidth, at the request of Safeguarding or Senior Leaders, or for any other reason deemed reasonable.

If a Staff member uses their own phone or device to take a picture or video for marketing purposes the media must be deleted immediately after transferring it to the college network. Transfer to the college network must happen in a timely fashion. This policy expects that staff transfer any photos from their devices on their next visit into college.

Staff are permitted to have college email accounts and cloud sync accounts setup on their personal devices however, these devices must be passcode locked, remain locked when not in use and have the ability to remote wipe the device if stolen or lost. Storage of college emails or Data on devices that do not support this functionality is not permitted.

Transfer of Data

The use of portable storage devices is prohibited on any JLCNET connected device, without prior authorisation from IT Services (for example, to collect CCTV footage).

The transfer of data out of the organisation must be done in a supported and pre-approved way. Please consult the data protection policy and the data protection officer regarding what data can be shared with whom.

During the transfer of data this policy specifies that a minimum encryption of AES-256 bit level is used. This should be used by securing the data into a password protected Zip file. The password and zip file must then be communicated using separate methods. IT Services produce a number of guides on how to do this.

JLC
IT SERVICES

Working from Home

A range of IT Services are available from home. This includes CEDAR, Google Classroom and Office 365.

The college also provides Azure Remote Desktop services and/or VPN for certain users.

When using services from home please take extra care. You must ensure your device has up to date anti-virus and malware protection.

We strongly encourage staff to use video conferencing services provided by Google (Google Meet/Classroom). These systems are secure and make it easier for us to keep you and your students safe.

You should always use passwords when setting up any form of online meeting and you must record the session if you are working with students.

The use of other video conferencing services is permitted but you must secure any video conference event with a passcode and ensure recording is enabled if you are working with students.

When working from home you may be using your own personal devices. Please refer to our GDPR and BYOD guidance document for a list of things you should and should not do with your own devices in relation to working from home.

When working from home, staff must ensure that no college data is available to other members of the household. Staff must ensure that screens are not visible through windows and that household occupants are not present in the room during any JLC meetings or online sessions.

Use of IT Equipment

There are a range of IT devices in college for users to use.

In some circumstances, users are allowed to book out a laptop computer, Chromebook iPad, etc. for use at home. This process is recorded and monitored by IT Services. Users borrowing devices are subject to the IT asset loan agreement. Users accept responsibility for any damage caused to devices whilst on loan and will reimburse the college for damage, up to the total replacement cost of the equipment. Users should take care of equipment they use. Users should report any non-functioning equipment to the IT Services team via the helpdesk or by emailing ithelpdesk@leggott.ac.uk.

Users are not permitted to remove any peripheral devices such as keyboards and mice or to open up machines for servicing. Users are not permitted to relocate IT assets without prior approval of IT Services.

Use of USB Memory sticks or other USB removable drives is not permitted on campus except in specialist areas. Users are encouraged to utilise the unlimited GoogleDrive storage space for accessing work remotely.

Users' private documents area (Drive H:) can only be accessed by the student owning the area. IT Services staff also have access to these areas for the purposes of IT support and backup.

Users are to store only college related data in this area. Users should not store any data (documents or images) that are of a personal nature.

IT Services staff will not go into a users file area unless a problem is identified, support is required, at the request of HR (for staff) or Safeguarding (for students), or a backup needs to be taken.

There are a range of curriculum applications installed across the college. Some applications are installed on all machines and some are restricted to particular areas.

Users are not permitted to access inappropriate content on any college connected devices, this includes personal devices connected to the guest networks. Inappropriate content is classified as anything illegal, harmful or upsetting to other students, staff or external individuals. Networks are monitored using multiple solutions that inspect network traffic and also keywords typed.

Users are reminded through a range of eSafety materials to be aware of the effects of digital harassment or bullying and the impact of sharing personal images with others either via direct messaging or social media platforms.

JLC
IT SERVICES

Loan of IT Equipment

Staff must not loan IT equipment to students (devices, chargers, peripherals) without permission from IT Services and appropriate paperwork being completed. Students must not assume chargers, devices or peripherals around college are available to borrow without permission from IT Services. All users must take reasonable care of all of JLCs assets and accept financial responsibility for any borrowed equipment, as outlined in the 1-2-1 loan forms.

Monitoring of Activity

IT Services staff have the ability to monitor user activity on the network and at any time on JLC owned devices, regardless of their location. Monitoring can take place without warning and record window activity, website history, application use, file save/deletion and any other activity carried out on the equipment.

Monitoring of activity on the network is designed to safeguard students, staff, and the college, particularly ensuring that sites cannot be accessed that may put students at risk of being radicalised. Further information on this can be found in the Safeguarding Policy.

Services

IT Helpdesk

The IT Helpdesk is located in front of the IT Services office in The Portal. Users can report to the desk for help and support for any IT related issue. Tickets must be logged using the iPad when approaching the desk.

Users can email ITHelpdesk@leggott.ac.uk to log a ticket. Users can also login to the IT Services Portal by following the links on the college website or by going to https://jlc-ithelpdesk.leggott.ac.uk/.

Logging into the IT Services Portal will provide access to recent tickets and help guides on performing common tasks. Users should search for help guides before logging a ticket, as a self-help guide may be available.

CEDAR

CEDAR is our primary CIS system for accessing student data from our CIS systems. Users can login to CEDAR using the link on the desktop of a college machine or by going to the Staff and Student Resources link on the college website.

CEDAR provides access to student's information and timetable information.

Remote Access

Access to Office 365 and Google Apps services are available from links on the college website or as links on the desktop of college devices.

Guidance for Remote Access

Users should be mindful of the security of the device they are using for accessing remote access services.

Users should ensure that the device they use to access these services has up to date security patches and antivirus software.

Users must ensure that all devices used to connect to remote services are free from malware and other credential stealing software. All devices used to access JLC services remotely must have a supported operating system installed with all security updates. Staff are required to adhere to the MAM policies in place when accessing JLC content through personal devices. This may require the installation of an app. This app allows JLC to see the following information:

- Device owner
- Device name
- Device serial number
- Device model, such as Google Pixel
- Device manufacturer, such as Microsoft
- Operating system and version, such as iOS 12.0.1
- Device IMEI
- App inventory and app names, such as Microsoft Word
- On personal devices, your organisation can only see your managed app inventory, which includes work and school apps.

JLC will never be able to see the following using the InTune Company Portal App:

- Calling and web browsing history
- Email and text messages
- Contacts
- Calendar
- Passwords
- Pictures, including what's in the photos app or camera roll

- Content of user created documents

When using JLC devices, please see "Monitoring of Activity".

When using college services remotely users are bound by college IT policies and should be mindful of the way in which they use remote services to ensure they still comply with all IT and general college policies.

Login information and location information are logged by some remote access systems.

Staff and students should remember that the security of their credentials is paramount considering the remote access capabilities of their accounts.

Assets and Asset Recording

IT Services log and record all assets purchased by the college.

Each asset is tagged with a barcode showing the asset ID number, smartwater (if appropriate) and a UV pen indicating the asset number and identifying the college the asset belongs to.

Asset information is recorded such as make, model, serial number and any configuration information needed by the IT Services team.

Assets may be assigned to a user if that user is the primary owner or user of that device. Devices that often have assigned users are portable devices (laptops, desktops, mobile phones) and specific devices used for the users job role (such as accessibility equipment).

An asset loan form will be used to log the asset to the user.

Users should not remove or alter the asset identification markings on any college owned asset.

Please see our Asset Management Procedures for more information on IT Asset Management.

Digital Signage

The college has a number of Digital Signage displays around the college. Users should pay particular attention to any college wide messages displayed as 'Urgent'.

Users can request specific information be shown on the displays by logging a ticket with the Marketing department.

Social Media Accounts

The college utilises various forms of social media and online marketing tools. Accounts in the name of John Leggott College must be setup by JLC IT Services. The team will create the necessary accounts and issue the username and password. It is prohibited to setup any account under the John Leggott College name that is not centrally managed by the college IT Services team.

This policy only applies to social media accounts used for the purpose of promoting JLC i.e. marketing accounts, departmental accounts. Personal social media accounts are covered by the Staff Code of Conduct.

Infrastructure

Backup and Disaster Recovery

A separate Backup and Disaster Recovery Procedure is in place. Brief information about our disaster recovery procedures is documented below.

Users should expect data stored on college systems to be backed up daily. This data is also copied offsite daily. These schedules may change during extended periods of college closure such as the summer holidays.

Users can request a copy of the current backup and retention schedule in effect at any time.

A Backup and Disaster Recovery procedure is in place which details the steps taken to recover from a disaster and the communication and priority methods used for recovery.

Internet Connectivity

The college has three methods of internet connectivity in the form of 1 x 10Gbps link and 2 x 1Gbps link.

Internet traffic can be routed via any connection due to demand or performance requirements.

Internet connectivity is filtered by an on-site firewall and filtering appliance and software. This appliance logs all internet traffic including the user requesting the content and the time they requested it. The secondary software also logs all keywords identified as harmful which are reviewed by Safeguarding and Wellbeing.

The following cloud services are used by the college and provided to users.

- Microsoft Office 365
- Google Apps for Education
- A web server for hosting web content
- 8x8 Cloud Telephony
- Adobe Creative Cloud
- Other cloud based SaaS solutions

Hardware
Dell are the main suppliers of hardware to the college.

Dell provides a range of support material specific to their devices. This support material can be found at support.dell.com. Users can contact IT Services for any support requirements relating to hardware.

Software
The college licences a range of software packages for installation on college machines.

Licences are for college use only and unless otherwise stated users are not permitted to install college software on their own devices.

Problem Management
A centralised IT Helpdesk is in place for logging of tickets and IT related issues. Both staff and student accounts have access to this cloud-hosted portal. Problems are resolved by any member of technical staff with escalation to the IT Manager if needed.

Change Management
Due to the small scale of our IT Services team there is no set change management procedure in place. Changes to the infrastructure are made as an when by IT Services Team members with approval from the IT Manager. The IT Manager has ultimate authority for changes and IT Services Team members are to approve major changes with the IT Manager beforehand.

Security
Aspects of IT security are covered throughout this document. Users must comply with the following:

- Use of strong passwords that meet the password policy.
- Use of college email accounts must not be used for personal uses, unless this is required by the service provider (UCAS, Staff discounts, etc.).
- MFA must be enabled for all services staff use (wherever this is supported by the 3rd party) and all JLC services that students use.
- Users should follow good GDPR practices including making sure digital and physical data is secured.
- When using personal devices, these must have supported operating systems installed and all available security updates installed.
- Staff must provide information to IT Services, when requested, about the systems they use on the John Leggott College network, or with John Leggott College credentials.
- Users should not knowingly introduce malware or vulnerabilities into the JLC network.

Users should comply with the following:

- Be mindful of all actions they undertake when using JLCs network or services.
- Consider if services used are fit for purpose, provided by a reputable company and secure in nature.
- Be aware of phishing and social engineering techniques that may be used against them.

IT Security at JLC is multifaceted and is made up from the following core principles:

- Strong passwords
    - IT Staff are required to use passwords with 16 characters and each password for each service must be unique.
    - Staff and students are encouraged to use strong passwords and SSO where possible.
- MFA
    - IT Staff are required to use MFA for as many services as it is available for. All core services are secured with MFA and remote access to servers is secured with MFA.
    - All staff and students are required to use MFA to access JLC services when off-site.
- Regular updates and patching

    - JLC follows strict update procedures. All security updates are installed within 2 weeks of release for all critical infrastructure (servers, firewalls, Wi-Fi infrastructure, etc.).
    - Client devices receive Windows Updates within 14 days of release. These are released by SCCM.
    - Client devices receive 3rd party security updates within 14 days of release. These are released by PatchMyPC via SCCM.
    - All security software is kept up-to-date automatically and checked by IT staff routinely.
- Use of modern anti-virus/malware solutions
    - Anti-malware, ant-ransomware and machine learning type software security is in use at JLC.
    - Backstop software is in place to protect against ransomware attacks.
- Next generation firewalls utilising IPS, AV, Web Filtering, DNS Filtering, and deep packet inspection
    - FortiGate firewalls are in use with all aspects of packet inspection enabled.
- Data encryption
    - Encryption of critical information is used, with backups encrypted and stored immutability.
- Secure network connectivity (802.1x)
    - Wi-Fi is secured using certificate based device credentials.
    - Network ports are secured with 802.1x port-based security.
- Staff phishing training
    - Staff are required to complete security and phishing training termly.
- Data backups (3-2-1)
    - Backups are taken daily and stored in 2 repositories (one offsite and immutable). Backups are also taken weekly and stored on an air-gapped storage device.
- Access control
    - Only IT Services staff hold administrative privileges for any IT service or device (from client device to servers. There is no access to any infrastructure to any non-IT Staff.
- Physical security
    - Only IT staff and necessary estates staff have physical access to critical infrastructure. This is protected by Paxton Net2 locks and any access attempts are logged with IT.
- Network monitoring
    - Network monitoring is performed by multiple tools (Zabbix, Roboshadow).

Cyber Security Response Procedure

If IT services, staff or students detect or notice a cyber security incident, they should notify the IT Manager or member of the IT Services team immediately.

IT Services will do the following upon suspicion or report of a cyber security incident:

1. Detection and Identification:

- Identify and verify the cybersecurity incident. It may involve unusual system behaviour, alerts from security tools, or reports from employees.
- Once identified that there has been an incident, SLT will be informed.

2. Immediate Containment:

- Isolate affected systems or networks to prevent further damage.
- Disconnect compromised devices from the network, if necessary.

3. Investigation and Analysis:

- Conduct a thorough investigation to determine the scope and nature of the incident.
- Gather evidence, logs, and other relevant information.
- Consult with cybersecurity experts if necessary.

4. Communication:

- Establish internal and external communication channels:
    - Notify senior management and legal counsel.
    - Communicate with law enforcement, if required.
    - Prepare a communication plan for employees, customers, and affected parties.
    - Notify the cyber insurance company.
    - Notify JISC Cyber Response team.

5. Mitigation:

- Implement measures to prevent a recurrence:
    - Apply security patches or updates to vulnerable systems.
    - Change compromised passwords.
    - Update security policies and procedures, if necessary.

6. Recovery:

- Develop a plan for recovering affected systems and data:
    - Restore systems from secure backups.
    - Test and validate the restoration process.

7. Legal and Regulatory Compliance:

- Ensure compliance with legal and regulatory requirements regarding data breach reporting and customer notification.

8. Documentation:

- Maintain detailed incident records, including actions taken, communication logs, and findings from the investigation.
- Prepare an incident report outlining the incident's cause, impact, and lessons learned.

9. Public Relations and Notification:

- Work with public relations and legal teams to communicate with the public and affected parties as necessary.
- Follow legal requirements and best practices for data breach notifications.

10. Post-Incident Review:

- Conduct a post-incident review to analyse the response and identify areas for improvement.
- Update policies and procedures based on lessons learned.

11. Training and Awareness:

- Provide training and awareness programs for employees to prevent similar incidents in the future.

12. Continuous Improvement:

- Continuously monitor and enhance security measures and incident response procedures to adapt to evolving threats.

13. End of Incident Response:

- Conclude the incident response process and return to normal operations.

14. Review and Update:

- Periodically review and update the incident response procedure to reflect changes in the threat landscape and the organisation's infrastructure.

Please also see the additional file RC Operational Response Plan.pdf.

Consequences

Users may be subject to college disciplinary procedures if they do not adhere to the guidelines in this policy.

Principal's Discretion

Where there is no statutory duty to comply the Principal reserves the right to apply their discretion in the undertaking of this policy.

JLC
IT SERVICES

IT Policy

May 2024

Please sign to confirm you have read and understood this policy.

Name	
Signature	
Date	

Please return this slip to IT Services