Wandsworth Lifelong Learning

Wandsworth Council

Cyber Security Policy



OCTOBER 2026

Aiming to improve the quality-of-life skills and employability of residents in the borough, making Wandsworth a vibrant and prosperous learning community.

Version	1
Original Policy issued:	October 2026
Reviewed:	October 2026
Next review date:	October 2027
Review cycle:	Annual, or sooner following a significant incident or change in requirements
Name originator/author:	Deputy Head of Lifelong Learning
Contact details:	yvonne.leung@richmondandwandsworth.gov.uk Reception: 020 8871 8055 I T: 020 8871 7211
Target Audience	All WCLL staff, subcontractors and authorised users; with specific requirements for examination staff

Designed and produced by Richmond and Wandsworth Design & Print. wdp@wandsworth.gov.uk CS1942S (10.26)

Contents

1	Introduction	3
2	Scope	3
3	Intent	3
4	Governance and Responsibilities	4
	- Head of Centre and Senior Leadership	4
	- Examinations Officer and System Owners	4
	- Managers, Staff and Subcontractors	4
	- Staff Responsibilities at a Glance	4
5	Identity, Account and Access Security	5
6	Secure Systems, Devices and Information	6
7	Examination and Awarding-Body Systems	6
8	Cyber Incident Reporting and Response	7
	- How to report	7
9	Awareness, Assurance and Review	8
	- Related policies and guidance	9

Cyber Security Policy

1 Introduction

Wandsworth Council Lifelong Learning (WCLL) relies on secure digital services to deliver learning, administer qualifications and examinations, and protect personal, confidential and assessment-related information. This policy sets out arrangements to protect the confidentiality, integrity and availability of systems and information, safeguard examination and awarding-body data, and reduce the risk and impact of cyber incidents.

The policy supports the Richmond & Wandsworth Better Service Partnership Information Security Handbook, associated information security policies and guidance, the Data Protection Policy, Acceptable Use Policy, Bring Your Own Device Policy, Business Communications Policy, business continuity arrangements, and security incident reporting processes. It also addresses the JCQ General Regulations for Approved Centres (effective from 1 September 2026) and JCQ guidance on cyber security.

2 Scope

This policy applies to all WCLL employees, temporary and agency staff, tutors, volunteers, subcontractors, partner staff and other authorised users who access council or WCLL devices, networks, cloud services, data, or examination and awarding-body systems. It applies whether work is undertaken at council premises, community venues, remotely, or through an approved bring-your-own-device arrangement.

Subcontractors and third parties must comply with applicable security and data protection requirements, use approved systems, report incidents promptly, and provide assurance of appropriate controls. Where examination activity is supported, provider policies must meet or exceed this policy and relevant JCQ requirements.

3 Intent

WCLL will manage cyber risk through clear accountability, secure configuration, controlled access, staff awareness, prompt incident reporting, tested recovery arrangements and continuous improvement. Security controls will be proportionate to risk and protect council services, learners, candidates, employees, partners, awarding bodies and the integrity of assessments.

As an approved examination centre, WCLL will maintain this policy for inspection, communicate it to relevant staff, review it at least annually or following significant incidents or changes in requirements, and retain evidence of annual cyber security awareness training for staff who access awarding-body systems.

Where council requirements, JCQ regulations, awarding-body instructions or contractual controls differ, WCLL will apply the most stringent requirement and seek advice from the council's Information Security Team, Data Protection Officer or awarding body where necessary.

4 Governance and Responsibilities

Head of Centre and Senior Leadership

The Head of Centre is accountable for compliance with JCQ regulations and for ensuring that sufficient resources, authority and oversight are in place. Senior leadership will approve this policy, receive assurance on training and incidents, and ensure that cyber security is integrated into examination contingency and business continuity arrangements.

Examinations Officer and System Owners

The Examinations Officer will maintain a current list of authorised users of awarding-body systems, coordinate access reviews, confirm annual training completion before access is granted or continued, and retain evidence for inspection. System and information owners will approve access according to role and promptly notify administrators when access must change or be removed.

Managers, Staff and Subcontractors

Managers must communicate this policy, monitor compliance and ensure leavers, movers and joiners are handled promptly. All users must follow council security instructions, complete required training, protect credentials and devices, use approved services, and report suspected incidents or vulnerabilities immediately. Subcontractors must provide equivalent assurance for their personnel and systems.

Staff Responsibilities at a Glance

Evidence principle	WCLL requirement
All staff and authorised users	Follow council and WCLL security requirements; use only approved devices, systems and storage; protect passwords and MFA credentials; complete required training; remain alert to phishing and social engineering; and report suspected incidents, vulnerabilities, lost devices or information immediately.
Staff accessing awarding-body systems	Complete cyber security training annually; use an individual authorised account and MFA where available; protect candidate and examination information; comply with JCQ and awarding-body instructions; and provide evidence of training completion for inspection.
Managers	Communicate this policy; ensure staff complete training; approve access according to role; notify account administrators promptly about starters, leavers and role changes; monitor compliance; and escalate concerns.
Examinations Officer	Maintain the authorised-user list for awarding-body systems; coordinate annual access reviews; verify annual training completion; retain inspection-ready evidence; and escalate actual or suspected examination-system incidents.

Head of Centre and senior leadership	Provide oversight and resources; approve and annually review the policy; assure JCQ compliance; monitor significant risks and incidents; and ensure examination contingency, business continuity and recovery arrangements are maintained and tested.
Subcontractors and third parties	Meet applicable council and WCLL security and data protection requirements and, where supporting examination activity, comply with relevant JCQ requirements. Relevant personnel must complete required cyber security training, use approved systems, protect WCLL and examination-related information, report security incidents promptly, and provide security assurance when requested.

5 Identity, Account and Access Security

- Each user must have an individual account. Shared credentials are prohibited unless a formally approved technical account is required and controlled.
- Access must be authorised before use, follow least-privilege and need-to-know principles, and be reviewed at least annually, following role changes, or when access is no longer required.
- Accounts must be disabled promptly when no longer required. Dormant, duplicate and unnecessary accounts must be removed.
- Strong, unique passwords or passphrases must be used and must not be reused, disclosed, stored insecurely or included in emails. Any password known or suspected to be compromised must be changed promptly.
- Secure account recovery options must be configured and maintained for relevant accounts. Connected applications linked to accounts or systems containing examination-related information must be regularly reviewed, with unauthorised or unnecessary applications removed promptly.
- Where available Multi-Factor Authentication (MFA) must be enabled for all accounts and systems containing examination-related information, including systems and interfaces that exchange information between awarding-body and centre systems. MFA prompts must never be approved unless initiated by the user.
- Where MFA is unavailable on a relevant centre system, an equivalent multi-layered security approach must combine strong login controls, restricted access, monitoring and secure storage to protect examination-related data.
- Security settings for accounts and systems containing examination-related information must be reviewed regularly and updated as necessary to reflect current security best practice, council requirements, JCQ regulations and awarding-body instructions.
- Privileged and administrator access must be limited, separately controlled and used only for authorised administrative tasks.

6 Secure Systems, Devices and Information

- Only council-approved and appropriately managed devices, software, cloud services and storage locations may be used for council or examination activity.
- Third-party and cloud suppliers must be subject to appropriate security and data-protection assurance. Where they support examination activity or process personal data, applicable contractual security controls must be in place, including a data processing agreement where required. Suppliers must report incidents affecting WCLL or examination-related information promptly.
- Devices and applications must be supported, securely configured, encrypted where required, protected by current anti-malware controls and updated promptly. Automatic locking must be enabled.
- WCLL will maintain a register of devices and user accounts used for examination and assessment purposes.
- Exam files, candidate data, credentials and other sensitive information must be stored and transmitted only through approved secure services, with access limited to authorised staff.
- Candidate registration details, including learner names, dates of birth and registration numbers, may be shared with authorised invigilators and other staff involved in examination administration. Council-authorised Microsoft 365 Outlook accounts may be used for this purpose, subject to council security requirements. Only information necessary for the task may be shared, and recipients must be verified before sending.
- Users must remain alert to phishing, malicious links, unexpected attachments, social engineering and fraudulent MFA prompts. Suspicious messages must be reported using Outlook's Report Message function and must not be forwarded to colleagues.
- Removable media must not be used unless authorised, encrypted and is considered to be necessary. Personal email, consumer file-sharing services and unapproved messaging or AI tools must not be used for council or examination information.
- Physical records, devices and screens must be protected from unauthorised viewing, loss or theft. Any loss of examination-related information or equipment must be reported immediately.
- Web filtering, monitoring, logging and protective controls will be applied by the council or approved service provider to block malicious activity, detect suspicious activity, and support investigation.

7 Examination and Awarding-Body Systems

Access to awarding-body systems and examination information is restricted to authorised staff with a legitimate role. Users must comply with JCQ regulations, awarding-body instructions and this policy.

- Annual cyber security training is mandatory for every member of staff who has access to an awarding-body online system.
- WCLL will retain evidence of completion for inspection. Evidence may include certificates, Learning Management System reports, paper checklists or spreadsheet-based records.

- Training must cover the topics specified in the JCQ General Regulations for Approved Centres, including strong and unique passwords, keeping account details confidential, the importance of Multi-Factor Authentication (MFA) and how to set up and use it for centre and awarding-body systems, awareness of social engineering and phishing, and prompt reporting of suspicious activity within a safe and supportive reporting culture.
- Access will not be granted or continued until the required annual cyber security training has been completed. Where a user has not completed the required training, their access will be withheld or suspended until completion is confirmed.
- Authorised staff must access awarding-body online systems in accordance with awarding-body security requirements. Where necessary, they must have access to a device that meets the awarding body's MFA requirements.
- Assessment administration systems and critical exam data must be included in business continuity and disaster recovery arrangements. Recovery processes will be tested at least annually and lessons recorded.
- Electronically produced candidate work must be backed up securely to protect against system corruption and cyberattacks. Back-up arrangements must use secure storage appropriate to the sensitivity and importance of the work. Where practicable, WCLL should maintain two separate back-ups, including one off-site or in the cloud with a reputable provider using robust security measures.
- Any actual or suspected compromise of an awarding-body online system must be reported immediately to the relevant awarding body in accordance with its instructions, and to the council through the applicable incident reporting process.

8 Cyber Incident Reporting and Response

Users must report actual or suspected cyber incidents without delay. Warning signs include:

- Suspicious emails, unexpected credential or Multi-Factor Authentication (MFA) prompts.
- Misdirected emails containing sensitive information.
- Unusual account activity or logins.
- Lost devices.
- Ransomware, service disruption and/or third-party compromise and,
- the loss or unauthorised disclosure of examination-related or personal information.

How to report

- Suspicious email not opened or interacted with: Use Outlook's Report Message function.
- Access, information or physical security concerns: Report through The Loop security incident and vulnerability process.
- Serious or unusual incidents: This includes suspected account compromise, interaction with a suspicious message, ransomware, service disruption, third-party compromise, loss or unauthorised disclosure of high-risk information. Contact the council's 24/7 Cyber Hotline on 01483 520 349 to log a technology security incident.

- Personal data breaches: follow the council's data protection breach procedure and notify the appropriate manager and Information Governance contacts immediately.
- Awarding-body systems: any actual or suspected compromise of an awarding-body online system must be reported immediately to the relevant body, as well as through the council's incident reporting process, in accordance with this section and the awarding body's instructions.

Users must not investigate incidents, delete relevant evidence, contact suspected attackers, pay a ransom or attempt recovery unless instructed. They must record what happened, preserve relevant evidence and follow instructions from the Cyber Hotline, Corporate IT, the Information Security Team, the Data Protection Officer, the Head of Centre and the relevant awarding body.

WCLL will coordinate containment, impact assessment, business continuity, recovery, required notifications, evidence preservation and lessons learned. Incidents affecting examinations will be managed to protect assessment integrity and candidates' interests.

9 Awareness, Assurance and Review

All staff must complete council-mandated information security and cyber security awareness training at induction and at the required refresher interval. Staff with access to awarding body systems must complete annual cyber security awareness training approved by the council, the NCSC, or an equivalent programme approved by WCLL as meeting current JCQ and relevant awarding body requirements. Managers and the Examinations Officer will monitor completion, follow up non-compliance and retain inspection-ready records.

Awareness activity will reinforce phishing reporting, social engineering awareness, account security, MFA, secure information handling, remote work, incident reporting and examination-specific responsibilities. Additional briefings or simulated exercises may be used where risk or incidents indicate a need. Training and awareness content will be reviewed periodically to reflect emerging cyber threats and changes to council, JCQ and awarding-body guidance.

Compliance will be monitored through access reviews, training records, device and account registers, incident trends, supplier assurance, recovery testing and internal checks. Material gaps will be recorded, assigned to an owner and tracked to completion.

This policy will be reviewed at least annually or following a significant cyber incident, material system or supplier change, audit finding, or change to council, JCQ, awarding-body, legal or regulatory requirements. The current approved version will be communicated to relevant staff and made available for inspection by JCQ and awarding-body representatives on request.

Related policies and guidance

- Richmond & Wandsworth Better Service Partnership Information Security Handbook and information security policies and guidance
- Council security incident and vulnerability reporting process and Cyber Hotline guidance
- Wandsworth Council Data Protection Policy and personal data breach procedure
- Acceptable Use, Bring Your Own Device and Business Communications policies
- WCLL examination contingency and business continuity arrangements
- JCQ General Regulations for Approved Centres 2026–27, JCQ Guidance for Centres on Cyber Security and the JCQ sample centre cyber security policy