Cyber Security Policy

For the attention of:	All Staff,
Produced by:	Group Executive Director Technology
Approved by:	CEO and Group Principal
Date of publication:	October 2025
Date of next review:	October 2027 (or following significant change)

WINDSOR FOREST COLLEGES GROUP

Vision, Purpose & Values

Our Vision

Our students will be recognised locally & nationally for their positive impact on the communities and industries in which they choose to work.

Our Purpose

To inspire our students to gain the skills, knowledge and behaviours they need to be resilient and thrive in an ever-changing world.

Our Values

Excellence: A culture of creativity, high expectations, ambition and aspiration

Respect: Showing fairness, courtesy and mutual respect to each other and our environment

Integrity: Honesty, openness and trust at the heart of College life

Diversity: Celebrating diversity and inclusivity as a key to our success

Contents

1. Introduction

The Windsor Forest Colleges Group (WFCG) is committed to safeguarding its information assets, IT systems and the personal data of students, staff and stakeholders from cyber threats. This policy sets out our approach to cyber security, aligns with our Business Impact Analysis (BIA) and outlines roles, responsibilities and compliance requirements. It supports our resilience planning for critical systems including Tribal EBS (MIS), MHR iTrent (HR), OpenAccounts/eBIS (Finance), Google Workspace, Microsoft Outlook/Teams, CPOMS, and the Individual Learner Profile (ILP).

2. Scope

This policy applies to all staff, students, governors, contractors and third parties who access WFCG's IT systems, networks and data. It covers all campuses, cloud-hosted services and on-premises infrastructure managed by WFCG.

3. Roles and Responsibilities

Roles and responsibilities are aligned with our BIA and disaster recovery framework:

Role	Responsibilities
CEO / Group Principal	Overall accountability for cyber security and incident response.
Group Executive Director Technology & Group Head of IT, Security and Infrastructure	Lead responsibility for cyber security strategy, implementation and oversight of the BIA.
IT Services Team	Implement technical controls, monitor systems, respond to incidents, manage access, backups and patching.
Data Protection Officer	Ensure GDPR/Data Protection compliance, oversee data breaches, report to ICO if required.
Senior Leadership Team & Governors	Oversight and assurance of cyber security and BIA alignment.

All Staff	Complete annual cyber training, follow policy, report incidents promptly.
Students & Users	Use IT systems responsibly, report concerns or suspicious activity.

4. Technical Security Measures

WFCG implements layered security measures consistent with NCSC guidance and tailored to our BIA-defined Recovery Objectives. These include:

- Firewalls, endpoint protection, and network segmentation
- Multi-factor authentication (MFA) for critical systems and remote access
- Regular patching, vulnerability management, and secure configurations
- Encrypted backups with termly restore testing
- Privileged Access Management (PAM) controls
- Cloud resilience (Microsoft 365, Google Workspace, SaaS systems)
- Rapid account deprovisioning for leavers

Minimum Recovery Time for internally managed applications and Recovery Point Objectives (per BIA):

System	RTO	RPO	Criticality
Tribal EBS (MIS)	24h	4h	Critical
OpenAccounts / eBIS (Finance)	24h	8h	High
Individual Learner Profile (ILP)	24h	4h	Medium

5. Incident Response Plan

All staff must report suspected security incidents immediately to IT Services via the Service Desk or directly to the Group Head of IT, Infrastructure & Security or Group Executive Director Technology. Incidents will be managed in line with the BIA Cyber Incident Playbook which includes scenarios such as ransomware, phishing/Business Email Compromise, DDoS, insider threats and patch failures.

The incident response process includes:

- Detection and logging
- Containment and eradication
- Recovery in line with BIA RTO/RPO targets
- External communications (NCSC, JISC CSIRT, ICO, awarding bodies as appropriate)
- Post-incident review and lessons learned

6. Staff Training and Awareness Responsibilities

All staff must complete mandatory annual cyber security training covering phishing, password hygiene, social engineering, and incident reporting. Specialist one to one training is required for system owners, safeguarding staff and exams staff. Training records are maintained by the Group Head of Digital Skills and Human Resources for audit purposes. Phishing simulations and awareness campaigns will be carried out every three weeks to reinforce vigilance.

Staff who fail phishing simulations will be required to undertake additional training, which may include one-to-one support. Two consecutive failures of phishing simulations may result in escalation to line management and will form part of performance management discussions.

7. Compliance and Auditing

This policy is aligned to UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and NCSC guidance. Annual review of the Cyber Security Policy is conducted alongside the Business Impact Analysis. Annual internal audits and disaster recovery simulations ensure policy compliance and readiness.

8. Related Policies and Standards

This Cyber Security Policy should be read in conjunction with the following Windsor Forest Colleges Group policies, procedures and frameworks:

- Business Impact Analysis (BIA) and Disaster Recovery Plan – defines critical systems, Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs).
- UK GDPR Policy – outlines requirements for lawful, fair and secure processing of personal data.
- Acceptable Use Policy (AUP) – sets rules for appropriate use of college IT resources, including personal/BYOD devices and cloud services.

- **Safeguarding Policy** – ensures that safeguarding considerations are embedded in all digital activities.
- **Document Retention Policy** – covers data classification, retention schedules and secure disposal.
- **Health & Safety and Estates Security Procedures** – include physical and environmental security measures (e.g. server room access).
- **HR Disciplinary Policy** – details consequences for policy noncompliance.

The Cyber Security Policy is also guided by external standards and frameworks, including:

- National Cyber Security Centre (NCSC) guidance for education
- Department for Education (DfE) Digital and Technology Standards for Cyber Security
- Information Commissioner's Office (ICO) guidance on data protection
- JISC and sectorwide cyber incident response recommendations

8.1 Digital and Technology Standards for Cyber Security

DfE Standard	Expectation	WFCG Current Compliance
Boundary protection (firewalls / filtering)	Robust firewall and filtering in place to protect systems and learners.	Enterprise grade WatchGuard firewalls deployed across campuses. Network segmentation referenced in BIA Scenario 3.
Malware protection	Anti-virus, anti-malware and endpoint protection across all devices.	Centralised Watchguard endpoint protection (AV/EDR) deployed across Group devices.

Secure configurations	Devices, servers, and services hardened to remove vulnerabilities.	Secure baseline builds applied, vulnerability scans carried out termly.
Access control	Unique user accounts, MFA for critical services, prompt deprovisioning of leavers.	MFA enabled for M365, Google Workspace, VPN. Leaver process built into HR/IT workflow.
Patch management	Regular updates with a tested change process.	Patch cycles monitored; failed patch scenario included in BIA playbook (Scenario 7).
Backups	Regular, encrypted, tested backups stored offline or in a separate environment.	Backups encrypted, stored cross-site. Termly restore tests mandated by BIA recommendations.
Incident response	Documented plan, roles defined, external reporting (NCSC, ICO, awarding bodies).	Cyber Incident Playbook in BIA (10 scenarios). Policy requires staff to report to IT Services; escalation to NCSC/JISC/ICO.
User awareness training	Annual staff training plus refreshers on phishing/social engineering.	Annual mandatory training, phishing simulations monthly. Additional 1:1 training/escalation for repeat failures.
Monitoring and logging	System activity logged, monitored, and reviewed.	Logs maintained across MIS/HR/Finance. Monitoring alerts integrated with IT Services escalation.

Physical security	Server rooms, comms rooms secured with controlled access.	Controlled access to Langley Data Centre; fire/flood scenario captured in BIA (Scenario 8).
Business continuity / disaster recovery	Critical systems must have defined RTOs and RPOs.	RTOs and RPOs documented in BIA (EBS, iTrent, Finance, CPOMS, etc.). Regular DR testing scheduled.

9. Supply Chain, Procurement and Third-Party Requirements

All new procurements, renewals, or third party services that handle College Group data must demonstrate compliance with recognised cyber security standards. As a minimum, suppliers must:

- Provide annual evidence of Cyber Essentials certification (or equivalent), and provide evidence of all in contract renewals.
- Request copies of annual internal audits of supporting infrastructure and systems
- Support **MFA**, encryption, and secure configuration as standard.
- Agree to data protection terms in line with **UK data protection laws** and the College Group's Data Protection Policy.
- Provide documented **business continuity and incident response processes** on an annual basis.
- Provide all data and encryption standards and certifications on an annual basis.
- Notify WFCG of any confirmed or suspected cyber incidents affecting their services within 8 hours.

Contracts and due diligence for critical systems (MIS, HR, Finance, safeguarding, cloud learning platforms) will include explicit clauses on cyber security, resilience, and termination/exit planning.

10. Policy Review

This policy will be reviewed annually by the Senior Leadership Team, informed by the Group's BIA and evolving cyber threat landscape. It must be formally approved by the CEO/Group Principal..