Access Control Policy

For the attention of:	All Staff
Produced by:	Group Exec Director of Technology & Group Head of IT, Infrstructure and Security
Approved by:	SLT
Date of publication:	April 2025
Date of next review:	April 2027

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. Purpose

This Access Control Policy establishes the framework for managing access to the information systems and data of The Windsor Forest colleges Group (WFCG). Its purpose is to ensure that access is granted appropriately, maintained securely, and removed in a timely fashion in accordance with the principles of data protection, confidentiality, integrity, and availability.

This policy is informed by best practice guidance from the UK National Cyber Security Centre (NCSC) and Jisc, and aligns with access control principles from peer educational institutions.

2. Scope

This policy applies to all individuals who access WFCG information systems, including staff, students, contractors, visitors and third parties. It covers all WFCG systems, whether hosted on-premises or in the cloud, including but not limited to:

- Outlook and Microsoft 365 services (email, calendars)
- Google Workspace for Education (Google Drive, Classroom, Docs, etc)
- Networked file storage and internal servers
- Cloud-based and managed hosted services
- Backup and disaster recovery infrastructure

3. Policy Statements

3.1. Principle of Least Privilage

Access to systems and data must be granted on a strictly "least privilege" basis. Users shall only be given the minimum level of access required to perform their dutires. This reduces the risk of unauthorised access and potential misuse.

3.2. Role-based and Tiered Access for IT Staff

IT staff are granted access to administrative systems based on clearly defined roles. Access is tiered to match job responsibilities, ensuring that elevated permissions are restricted to those who require them via separate admin specific accounts.

3.3. Access Approvals

All user access must be authorised before being granted:

Access to a staff email account or staff network drive must be approved by either:

- Two members of the Senior Leadership Team (SLT), or
- One SLT member and the user's line manager

- Privilaged access (e.g. administrative rights) requires written authorisation from an SLT member and the relevant system owner or manager.

3.4. Account Provisioning and Deprovisioning

User accounts are created based on formal onboarding processes (e.g. HR or enrolment records). Access rights are assigned according to role. When users change roles or leave the organisation, access must be reviewed and removed or adjusted promptly.

Dormant or inactive accounts will be disabled and reviewed regularly.

3.5. Authentication and MFA

All users must authenticate using unique credentials. Multi-factor authentication (MFA) is mandatory for staff and students on systems that support it, particularly for email, cloud storage, and administrative portals.

3.6. Shared and Service Accounts

Shared user accounts are not permitted. Service accounts (used by systems, not individuals) must be strictly controlled, uniquely identifiable, and reviewed regularly. Access to services accounts must follow the same principles of least privilege.

3.7. Access Control for Backups

Access to backup systems is limited to authorised IT personnel. Backup systems must be logically or physically segregated from production environments. Administrative access to backup solutions requires MFA and approval from the Group Head of IT or equivalent. Restore actions must be documented and follow proper authorisation protocols.

3.8. System Segmentation and Role Controls

Systems must enforce access controls via directory groups, roles, or access control lists. Role-based access control (RBAC) should be used wherever possible to streamline permissions and ensure least privilege. Access reviews must be conducted regularly to ensure accuracy.

3.9. Third-Party Access

Third parties must be granted access only via named accounts, with specific roles, and time-bound where possible. All third-party access must be authorised by an internal sponsor, reviewed regularly, and monitored.

4. Roles & Responsibilities

- SLT: oversees strategic approval of access to sensitive systems
- Line managers: authorise standard access for team members
- HR: notify IT of new starters, leavers or role changes
- IT Services: implement and enforce technical access controls, provision accounts, and monitor for misuse
- System/Data Owners: define and review access to their respective systems and datasets
- All Users: Maintain password security, report suspected security incidents, and use access appropriately

5. Monitoring and Audit

Access to systems is monitored and logged. IT Security will periodically review access logs and account privileges. Any irregularities will be investigated and may lead to disciplinary procedures.

Formal access reviews must be conducted at least annually by system owners and line managers. Compliance with this policy is subject to internal audit.

6. Training and Awareness

All staff and students must be aware of and comply with access control requirements. Security awareness training will include guidance on appropriate access use and safeguarding of credentials.

7. Review and Maintenance

This policy is reviewed annually or upon significant changes to IT systems or regulatory requirements. Changes will be approved by the SLT.

8. References

– NCSC: “Principle of Least Privilege” Guidance
– NCSC: “Access Control” Good Practice
– Jisc: Cyber Security Posture and Network Access Control Recommendations