EDA COLLEGE

EDUCATE I DEVELOP I ACHIEVE

IT Security and Cyber Security Policy[1]

Version Control/History

Title	IT Security and Cyber Security Policy
Reference	EDA-IG-ITSEC-01
Version	1.0
Approved by	Academic Board, EDA College
Date of Approval	August 2025
Effective Date	August 2025
Next Review Date	Annual review; full policy reviews every two years or sooner if required by changes in law, regulation or threat landscape
Owner	Manager of IT and Information Security
Applies To	All staff, governors, contractors, consultants, partners, agents, students and any other person accessing, using or supporting the College's information systems, data or networks, regardless of location or device
Classification	Public (with restricted operational annexes)

[1] *Aligned with the UK GDPR and Data Protection Act 2018, the Computer Misuse Act 1990, the Network and Information Systems Regulations 2018, the OfS Regulatory Framework, the NCSC Cyber Assessment Framework, Cyber Essentials and ISO/IEC 27001:2022*

Contents

1. Policy Statement

EDA College ("the College") is committed to protecting the confidentiality, integrity and availability of the information it holds, processes and transmits, and to safeguarding the IT systems, networks and digital services that underpin teaching, learning, research, administration and student support. The College recognises that information is a critical asset of the institution, and that strong information security and cyber security arrangements are fundamental to maintaining the trust of students, staff, regulators, awarding bodies, partners and the wider public.

This IT Security and Cyber Security Policy sets out the College's overarching framework for managing information and cyber risk in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the Computer Misuse Act 1990, the Network and Information Systems Regulations 2018 (where applicable), the Privacy and Electronic Communications Regulations 2003, the Higher Education and Research Act 2017, the Office for Students (OfS) Regulatory Framework, the NCSC Cyber Assessment Framework, Cyber Essentials and Cyber Essentials Plus, and the controls set out in ISO/IEC 27001:2022 and ISO/IEC 27002:2022. It works alongside the College's Data Protection Policy, Records Management and Retention Policy, Acceptable Use of IT Policy, Business Continuity and Disaster Recovery Plan and Risk Management Policy.

The Academic Board approves this policy and is ultimately accountable for the College's information security posture. The Manager of IT and Information Security / Chief Information Security Officer (CISO) is responsible for its implementation, monitoring and continuous improvement.

2. Purpose

The purpose of this policy is to:

- Establish a clear, consistent and risk-based approach to information security and cyber security across the College.
- Define the principles, controls and behaviours that protect the confidentiality, integrity and availability of College information and systems.
- Set out roles, responsibilities and accountabilities, including for the Board, the Senior Leadership Team, the CISO, the Data Protection Officer, Information Asset Owners, IT staff, line managers and all users.
- Support compliance with the UK GDPR principle of integrity and confidentiality (Article 5(1)(f)) and the security of processing requirement (Article 32), including appropriate technical and organisational measures.
- Demonstrate to the OfS, awarding bodies, validating partners, professional, statutory and regulatory bodies (PSRBs), funders, students and staff that the College manages information and cyber risk to a recognised standard.
- Reduce the likelihood and impact of cyber incidents, data breaches, fraud, ransomware, denial-of-service and other threats.
- Embed a culture of security awareness and shared responsibility across the College community.

3. Scope

This policy applies to all information created, received, processed, stored or transmitted by, or on behalf of, the College, regardless of format (electronic, paper, audio, video, image), location (College premises, cloud services, home, third-party premises) or device (College-owned, personally-owned or third-party).

It applies to all employees, members of the Board and committees, contractors, consultants, agency workers, agents, partners, volunteers, students and any other person who has been granted access to College information, IT systems or networks ("users").

It covers all information processing facilities owned, leased, hosted or operated by the College, including end-user devices, servers, networks, virtual environments, cloud platforms (Software as a Service, Platform as a Service and Infrastructure as a Service), the Virtual Learning Environment (VLE), email and collaboration tools, telephony, building management and access control systems, CCTV, payment systems, and any other system that creates, processes, stores or transmits College information.

4. Legal, Regulatory and Sector Framework

This policy gives effect to, and should be read consistently with, the following statutory, regulatory and good-practice frameworks:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including Article 5(1)(f) (integrity and confidentiality) and Article 32 (security of processing).
- Computer Misuse Act 1990, including offences of unauthorised access, unauthorised modification and making, supplying or obtaining articles for use in computer misuse offences.
- Network and Information Systems Regulations 2018 (NIS Regulations) where applicable to relevant digital service providers and operators of essential services.
- Privacy and Electronic Communications Regulations 2003 (PECR) for electronic marketing, cookies and similar technologies.
- Investigatory Powers Act 2016 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, where the College intercepts or monitors communications.
- Regulation of Investigatory Powers Act 2000 (RIPA), where applicable.
- Higher Education and Research Act 2017 and the OfS Regulatory Framework, including Conditions B1–B5 (quality and standards), C3 (student protection), E1 (public interest governance), E2 (management and governance) and (where applicable) E6 (cooperation with the OfS) and reportable events guidance.
- Counter-Terrorism and Security Act 2015 (Prevent duty) where information systems are used to support compliance.
- Equality Act 2010, including in respect of accessible security controls and reasonable adjustments.
- Companies Act 2006, in respect of accounting records and statutory registers.
- Bribery Act 2010, Modern Slavery Act 2015 and Fraud Act 2006.

- UKVI Sponsor Guidance for Worker and Student sponsors (record-keeping and access controls for compliance data).
- Payment Card Industry Data Security Standard (PCI DSS) where the College processes, stores or transmits cardholder data.
- ISO/IEC 27001:2022 – Information security management systems.
- ISO/IEC 27002:2022 – Information security controls.
- ISO 22301:2019 – Business continuity management systems.
- Cyber Essentials and Cyber Essentials Plus (NCSC / IASME).
- NCSC Cyber Assessment Framework (CAF) and 10 Steps to Cyber Security.
- Jisc guidance for higher and further education, including the Jisc Acceptable Use Policy and the Janet Security Policy.
- ICO codes of practice and guidance, including the Employment Practices Code and the CCTV Code of Practice.
- Awarding body, validating partner and PSRB information security requirements where applicable.

5. Definitions

For the purposes of this policy, the following definitions apply:

5.1 Information

Any data, knowledge or content held by the College in any format, whether structured (e.g. databases) or unstructured (e.g. documents, emails).

5.2 Information Asset

An identifiable body of information, system, application or service of value to the College (for example, the student record system, the finance system, the VLE, personnel files).

5.3 Information Asset Owner (IAO)

A senior member of staff accountable for the security, availability and lawful use of an information asset.

5.4 Confidentiality

Ensuring that information is accessible only to those authorised to have access.

5.5 Integrity

Safeguarding the accuracy and completeness of information and processing methods.

5.6 Availability

Ensuring that authorised users have access to information and associated assets when required.

5.7 Cyber Incident

Any event that has, or may have, an adverse effect on the confidentiality, integrity or availability of the College's information systems or data, including malware, ransomware, phishing, account compromise, denial-of-service, data exfiltration and unauthorised access.

5.8 Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5.9 User

Any individual authorised to access College information or systems, including staff, governors, contractors, agents, students and visitors.

5.10 End-User Device

Any device used to access College information, including desktops, laptops, tablets, smartphones, thin clients and removable media.

5.11 Cloud Service

Any IT service delivered over the internet by a third party (Software as a Service, Platform as a Service or Infrastructure as a Service).

5.12 Privileged Account

An account with elevated rights to administer systems, applications, networks or data (for example, domain administrator, database administrator, root).

6. Roles and Responsibilities

6.1 Academic Board

The Board has ultimate accountability for information and cyber security at the College. The Board:

- Approves this policy and the College's Information Security Management System (ISMS) framework.
- Receives at least annual reports on information and cyber risk, key incidents, audit findings and the effectiveness of controls.
- Considers cyber risk as part of the principal risk register and ensures the risk appetite is articulated and observed.
- Approves significant investment in information security capability and any acceptance of residual risk above tolerance.

6.2 Audit and Risk Committee

The Audit and Risk Committee provides independent oversight of the College's information and cyber security arrangements, including the effectiveness of internal controls, the risk register, audit findings and major incident lessons learned. It receives reports from internal and external audit and from the CISO.

6.3 Senior Leadership Team (SLT)

The SLT, led by the Principal/Chief Executive, is responsible for ensuring this policy is implemented within their areas, that adequate resources are made available, and that information and cyber risk is integrated into operational and strategic decision-making.

6.4 Manager of IT and Information Security / Chief Information Security Officer (CISO)

The CISO (or equivalent senior officer) is the policy owner and is responsible for:

- Day-to-day leadership of information and cyber security across the College.
- Maintaining the ISMS and the suite of underpinning standards, procedures and guidelines.
- Coordinating the response to cyber incidents and personal data breaches with the DPO and SLT.
- Reporting to the SLT, the Audit and Risk Committee and the Board.
- Liaising with the NCSC, Jisc, ICO, Action Fraud, law enforcement and other external bodies as required.

6.5 Data Protection Officer (DPO)

The DPO has responsibility for compliance with the UK GDPR and the Data Protection Act 2018, including the security of personal data, and works closely with the CISO on data protection by design and by default, DPIAs, breach assessment and notification.

6.6 Information Asset Owners (IAOs)

IAOs are accountable for the information assets within their portfolio. They:

- Maintain an up-to-date Information Asset Register entry for their assets, including classification, retention and lawful basis.
- Authorise access in line with the principle of least privilege.
- Sponsor risk assessments, DPIAs and reviews of supplier security.
- Report incidents and near misses promptly to the IT Service Desk and the CISO/DPO.

6.7 IT and Digital Services Team

IT staff implement and operate technical controls, including identity and access management, network security, endpoint protection, vulnerability management, monitoring, logging and backups. They follow agreed change management and configuration management processes and maintain documented operating procedures.

6.8 Line Managers

Line managers ensure that staff and contractors in their teams understand and comply with this policy, complete required training, hold only the access they need, and return equipment and revoke access promptly on changes of role or leaving.

6.9 All Users

All users are responsible for protecting College information and systems by complying with this policy, the Acceptable Use of IT Policy, the Data Protection Policy and related procedures, completing mandatory training, using strong authentication, reporting incidents promptly, and exercising due care when handling information.

7. Information Security Principles

The College's approach to information and cyber security is based on the following principles:

1. Risk-based: Controls are proportionate to the value of the information asset, the threat landscape, the likelihood and impact of incidents, and the College's risk appetite.
2. Defence in depth: Multiple, layered controls are used so that the failure of any single control does not result in compromise.

3. Least privilege: Users, processes and systems are granted only the minimum access necessary to perform their function, and only for as long as needed.
4. Need to know: Information is shared on the basis of demonstrable need, consistent with classification.
5. Secure by design and by default: Security and privacy requirements are embedded from the earliest stages of design, procurement and development, and the most secure settings are applied by default.
6. Accountability: Roles, responsibilities and decisions are clearly assigned, documented and auditable.
7. Continuous improvement: The ISMS is monitored, measured, reviewed and improved using a Plan–Do–Check–Act cycle aligned to ISO/IEC 27001.
8. Transparency and proportionality: Users are informed about how their information and activity may be monitored, in line with the UK GDPR, the Investigatory Powers Act 2016 and the ICO Employment Practices Code.

8. Risk Management Approach

The College manages information and cyber risk in accordance with the Risk Management Policy, ISO/IEC 27005 and the NCSC Cyber Assessment Framework. The CISO maintains an information security risk register that identifies threats, vulnerabilities, likelihood, impact and treatment.

Risks are assessed at least annually, and on:

- Procurement or significant change to an information system.
- Material changes to business processes or working practices (e.g. new partnerships, expansion of remote working).
- Identification of a new or emerging threat (e.g. through NCSC, Jisc CSIRT or industry advisories).
- Following a significant incident or near miss.

Treatment options include avoid, reduce, transfer and accept. Acceptance of risk above tolerance requires documented authorisation by the SLT and, for significant residual risk, the Board.

9. Asset Management and Classification

9.1 Information Asset Register

The College maintains an Information Asset Register documenting key information assets, their owners, location, classification, retention period and lawful basis (where personal data are involved). The register is reviewed at least annually.

9.2 Information Classification

Information is classified to indicate the level of protection required:

Classification	Description	Examples
PUBLIC	Information intended for public release; unauthorised disclosure presents minimal risk.	Marketing materials, published policies, course information.
INTERNAL	Information for general internal use; not for unrestricted external release.	Internal communications, organisational charts, draft documents.
CONFIDENTIAL	Information whose unauthorised disclosure could cause material harm to the College, an individual or a third party.	Personnel files, student records, financial accounts, internal investigations.
RESTRICTED	Highly sensitive information whose unauthorised disclosure could cause significant or severe harm.	Special category personal data, safeguarding records, board reserved business, security configurations, cryptographic keys.

Information must be handled, stored, transmitted and disposed of in accordance with its classification, as set out in the Information Handling Standard.

9.3 Removable Media and Hardware

Removable media (USB drives, external disks, optical media) are discouraged for College information. Where unavoidable, they must be College-issued, encrypted to AES-256 (or equivalent), inventoried and securely erased or destroyed at end of life. Hardware containing College data must be sanitised in line with NCSC guidance before disposal, reuse or return to a leasing company; certificates of destruction are retained.

10. Access Control and Identity Management

10.1 User Accounts and Joiners/Movers/Leavers

Each user is issued with a uniquely identifiable account. Generic and shared accounts are prohibited except where there is a documented operational necessity, in which case enhanced controls apply. Joiner, mover and leaver processes are agreed with HR and Academic Registry to ensure access is created, modified or revoked promptly and accurately. Access reviews are performed by IAOs at least every six months for systems containing CONFIDENTIAL or RESTRICTED information.

10.2 Authentication

Strong authentication is enforced for all users:

- Passwords / passphrases meet the NCSC password guidance (length over complexity, banned common-password list, no forced periodic resets unless compromise is suspected).
- Multi-Factor Authentication (MFA) is required for all remote access, all access to email and collaboration platforms, all administrative access, and all access to systems containing CONFIDENTIAL or RESTRICTED information.
- Single Sign-On (SSO) and federated identity are preferred and are configured with conditional access policies covering location, device posture and risk level.

- Service and machine accounts use strong, vaulted credentials, are non-interactive where possible, and are owned by an identifiable team.

10.3 Privileged Access Management

Privileged accounts are kept to the minimum necessary, are separate from standard user accounts, are subject to MFA, just-in-time elevation where feasible, recording of administrative sessions for sensitive systems, and quarterly review by the CISO. Default credentials are changed before any system enters service.

11. Endpoint, Server and Network Security

11.1 Secure Configuration

All endpoints, servers and network devices are configured to documented secure baselines aligned to NCSC and vendor guidance. Unnecessary services, accounts and software are removed; default passwords are changed; auto-run and auto-play are disabled where not required; firewalls are enabled.

11.2 Patch and Vulnerability Management

Critical and high-severity security patches are applied within 14 days of release, and other patches in line with the Patch Management Standard. Internet-facing systems are scanned for vulnerabilities at least monthly; internal systems at least quarterly. Penetration testing is performed at least annually and after material changes. Unsupported software is removed or formally risk-accepted with compensating controls.

11.3 Malware and Endpoint Protection

All endpoints and servers run College-managed endpoint detection and response (EDR) or anti-malware software with real-time protection, automatic updates and central reporting. Application allow-listing or equivalent execution control is implemented on high-risk systems. Removable media protection and disk encryption (full-volume) are enabled on all College mobile devices and laptops.

11.4 Network Security

The College operates a defended network architecture including:

- Perimeter and host-based firewalls with default-deny rule sets.
- Segmentation between user, server, management, guest, payment, IoT/OT and student-facing networks.
- Secure remote access via Zero Trust Network Access or VPN with MFA and device health checks.
- Wireless networks using WPA3 (or WPA2-Enterprise as a minimum) with strong key management; guest networks isolated from corporate resources.
- DNS filtering and protective DNS (such as the NCSC Protective DNS service or equivalent).
- Boundary and email filtering for malware, phishing, spam and impersonation, including SPF, DKIM and DMARC.

12. Cyber Essentials Controls

The College maintains certification or self-assessment alignment to Cyber Essentials, and works towards Cyber Essentials Plus where required by funders, partners or risk. The five technical controls are operated continuously:

9. Firewalls – boundary and host firewalls configured to a documented standard.
10. Secure configuration – hardened, baselined builds for endpoints, servers and cloud tenants.
11. Security update management – timely patching and removal of unsupported software.
12. User access control – unique accounts, least privilege, MFA, privileged access management.
13. Malware protection – EDR/anti-malware, application control and email/web filtering.

Where the College participates in research, partnerships or supply chains that require additional assurance (e.g. NCSC Cyber Assessment Framework outcomes, IASME Governance, ISO/IEC 27001 certification), the CISO ensures that the relevant controls are in place and evidenced.

13. Email, Web and Cloud Security

Email and collaboration platforms are configured to provide:

- Anti-phishing, anti-malware and anti-impersonation protection, including sandboxing of attachments and time-of-click URL rewriting.
- SPF, DKIM and DMARC records for all College sending domains, with DMARC progressing to a reject policy.
- External sender warning banners and configurable mailbox security settings.
- Encryption in transit (TLS 1.2 or higher) and, where appropriate, message-level encryption.

Cloud services are procured and operated under the Third-Party Security Standard. Each cloud service is subject to a documented assessment covering data residency, encryption, access management, logging, supplier security certifications (e.g. ISO/IEC 27001, SOC 2 Type II), exit and portability arrangements, and alignment with the UK GDPR (including international transfers using appropriate safeguards). Tenant-level configuration is reviewed regularly using cloud security posture management tooling.

14. Cryptography and Key Management

The College uses cryptography to protect the confidentiality and integrity of information at rest and in transit:

- All College mobile devices, laptops and removable media use full-volume encryption (e.g. BitLocker, FileVault) with keys escrowed centrally.
- CONFIDENTIAL and RESTRICTED information transferred outside the College is encrypted in transit (TLS 1.2 or higher) and, where appropriate, in the message or file (e.g. AES-256).
- Server and storage encryption is enabled where supported by the platform.
- Cryptographic keys, certificates and secrets are managed using approved key management systems and secret stores; private keys and tokens are never embedded in source code or shared by email.
- Algorithms and key lengths follow current NCSC and NIST guidance; deprecated algorithms (e.g. SSL, early TLS, MD5, SHA-1) are not used.

15. Secure Development, Change and System Acquisition

Where the College commissions, develops or significantly customises software (in-house or by third parties):

- Security and privacy requirements are defined at design stage, including UK GDPR data protection by design and by default.
- Development follows a documented secure development lifecycle (e.g. OWASP ASVS, NCSC secure development guidance).
- Code is version-controlled, peer-reviewed and subject to static and dynamic analysis where appropriate; dependencies are scanned and managed.
- Production data is not used in development or test environments unless anonymised, pseudonymised or otherwise protected in line with the Data Protection Policy.
- All material changes are subject to the Change Management Standard, including risk assessment, testing, approval, rollback planning and post-implementation review.
- Acceptance into service requires evidence of secure configuration, vulnerability testing, documentation, monitoring, backup and an Information Asset Register entry.

16. Third-Party and Supplier Security

The College recognises that a substantial proportion of cyber risk arises from suppliers and partners. All third parties that process College information or connect to College systems must:

- Be assessed for security and data protection maturity proportionate to the criticality and sensitivity of the engagement.
- Sign contractual terms incorporating the College's data protection and information security clauses, including UK GDPR Article 28 controller-processor terms where applicable.
- Provide evidence of recognised certifications or assurance (e.g. Cyber Essentials, Cyber Essentials Plus, ISO/IEC 27001, SOC 2) where appropriate.
- Permit audit, monitoring and incident notification within agreed timescales.
- Comply with the College's Acceptable Use of IT Policy and any system-specific security requirements when accessing College networks.

Material suppliers are subject to ongoing assurance, including annual review of certifications, incident history and changes to subprocessors. International transfers of personal data require an appropriate transfer mechanism (e.g. Adequacy Regulations, IDTA, UK Addendum to the EU SCCs) and a Transfer Risk Assessment.

17. Physical and Environmental Security

Physical security supports information security:

- Server rooms, communications cabinets and data centres are restricted to authorised personnel, with access logged and reviewed.
- Visitors are signed in, escorted as appropriate and their access to College systems is limited to that necessary.

- Clean desk and clear screen practices apply, particularly in areas where CONFIDENTIAL or RESTRICTED information is handled.
- Equipment is protected from environmental hazards (fire, flood, power loss, overheating) and supported by uninterruptible power and surge protection where critical.
- Disposal of equipment and media follows secure sanitisation procedures aligned to NCSC guidance, with certificates of destruction retained.

18. Acceptable Use, BYOD, Remote and Hybrid Working

All users must comply with the Acceptable Use of IT Policy, which sets out permitted and prohibited activities, monitoring arrangements and expectations of professional behaviour. In particular:

- College information must not be stored on personal storage, personal email or unsanctioned cloud services (“shadow IT”).
- Personally-owned devices used to access College information must comply with the Bring Your Own Device (BYOD) Procedure, including device enrolment, encryption, screen lock, supported operating system, EDR/anti-malware where relevant, and selective remote wipe.
- Remote and hybrid working follows the Remote Working Standard, including secure home network practice, use of approved collaboration tools, and avoidance of overlooking in public spaces.
- Use of generative AI and similar emerging technologies follows the College’s Responsible AI Use Standard, which prohibits the input of CONFIDENTIAL or RESTRICTED data into public AI services without prior approval.

19. Data Protection and Privacy by Design

This policy supports compliance with the UK GDPR and the Data Protection Act 2018. Personal data is processed in line with the Data Protection Policy, with security controls calibrated to the sensitivity of the data and the risks to data subjects.

Data Protection Impact Assessments (DPIAs) are completed for high-risk processing, including new systems handling personal data, large-scale processing, special category data and processing involving novel technologies. The DPO and CISO collaborate on DPIA reviews to ensure technical and organisational measures are appropriate under Article 32 UK GDPR.

Personal data breaches are managed in accordance with the Data Protection Policy and the Personal Data Breach Procedure, including assessment against the 72-hour ICO notification threshold and notification to data subjects where there is a high risk to their rights and freedoms.

20. Backup, Resilience and Disaster Recovery

The College maintains backup and recovery arrangements proportionate to the criticality of its information assets:

- Critical systems are backed up at least daily, with regular testing of restoration; backups follow a 3-2-1 strategy (three copies, two media types, one off-site/immutable copy).
- Backups containing personal data are encrypted, access-controlled and retained in line with the Records Management and Retention Policy.

- Immutable, isolated or air-gapped backups are maintained for systems most exposed to ransomware risk.
- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are documented for critical systems and tested in line with the Business Continuity and Disaster Recovery Plan.
- Business continuity exercises, including cyber incident scenarios, are conducted at least annually.

21. Logging, Monitoring and Threat Intelligence

The College captures and reviews security-relevant events to detect, investigate and respond to incidents:

- Security event logs from endpoints, servers, identity providers, firewalls, cloud platforms and key applications are forwarded to a central Security Information and Event Management (SIEM) capability or equivalent monitoring service.
- Logs are protected from unauthorised access and tampering, retained for a minimum of 12 months (longer where required for forensic, legal or regulatory purposes) and synchronised to a reliable time source.
- Detection use cases are tuned to the College's threat profile and reviewed at least quarterly.
- The College subscribes to threat intelligence feeds (including NCSC, Jisc CSIRT and sector advisories) and acts on alerts proportionately.
- Monitoring of users' use of College systems is conducted lawfully and transparently, in line with this policy, the Acceptable Use of IT Policy, the Data Protection Policy and the ICO Employment Practices Code.

22. Incident Management and Reporting

All users must report suspected information security or cyber incidents promptly to the IT Service Desk, the CISO or the DPO, in accordance with the Incident Response Plan. The College adopts a structured incident management lifecycle aligned to NCSC guidance and ISO/IEC 27035:

- ❖ Identification – reporting and triage.
- ❖ Containment – limiting the scope and impact.
- ❖ Eradication – removing the cause.
- ❖ Recovery – restoring affected services.
- ❖ Lessons learned – post-incident review and improvement.

Incidents are categorised by severity. Major incidents are escalated to the SLT, the Chair of the Board and, where relevant, the OfS as a reportable event under the OfS reportable events guidance. Personal data breaches that are likely to result in a risk to the rights and freedoms of natural persons are notified to the ICO within 72 hours of becoming aware. The College also notifies, where applicable, awarding bodies, validating partners, UKVI, funders, insurers, Action Fraud, the police and the NCSC.

The College maintains a register of all reported incidents, including near misses, and analyses trends to inform improvement. Disclosure of incidents to the College community is handled in line with the Communications Plan and is consistent with regulatory and legal obligations.

23. Training, Awareness and Culture

All staff and contractors complete information security and data protection awareness training at induction and at least annually thereafter. Role-based training is provided for those with elevated responsibilities, including IT staff, IAOs, the SLT, the Board and high-risk roles such as finance and HR.

The College runs an ongoing awareness programme that includes phishing simulations, intranet articles, briefings and exercises. Awareness materials are accessible and inclusive, in line with the Equality Diversity and Inclusion Policy and the Accessibility Statement.

Students receive guidance on safe and responsible use of College systems, online safety, account security, data protection and the implications of the Computer Misuse Act 1990 and the Acceptable Use of IT Policy. The College works with the Students' Union and Student Representatives to promote a positive security culture.

24. Compliance, Audit and Assurance

The College demonstrates the effectiveness of its information and cyber security arrangements through:

- Self-assessment against the Cyber Essentials and (as applicable) Cyber Essentials Plus controls, the NCSC Cyber Assessment Framework and the ISO/IEC 27001 control set.
- Internal audit reviews informed by the risk-based audit plan.
- External penetration testing and red/blue team exercises.
- Supplier assurance reviews and contract compliance checks.
- Reporting to the SLT, the Audit and Risk Committee and the Board on key indicators (e.g. patch compliance, MFA coverage, training completion, phishing test results, incident volumes and severity).

Where audit, regulatory or assurance findings identify deficiencies, the CISO ensures that remediation is planned, tracked and reported, with timescales proportionate to risk.

25. Breach of Policy

Breaches of this policy may compromise the security, integrity or availability of College information and systems and may expose the College and individuals to legal, regulatory, financial or reputational harm. Suspected breaches are investigated proportionately.

Failure to comply with this policy may result in:

- For staff: action under the Disciplinary Procedure, up to and including dismissal in cases of gross misconduct, and referral to professional bodies where applicable.
- For students: action under the Student Disciplinary Procedure and, where appropriate, the Fitness to Practise or Academic Misconduct procedures.

- For contractors and partners: termination of access, contractual remedies and recovery of losses.
- For all parties: referral to law enforcement where the conduct may constitute a criminal offence under the Computer Misuse Act 1990, the Fraud Act 2006, the Data Protection Act 2018 or other relevant legislation.

26. Related Policies and Documents

- Acceptable Use of IT Policy
- Data Protection Policy
- Records Management and Retention Policy
- Freedom of Information Policy
- Bring Your Own Device (BYOD) Procedure
- Remote Working Standard
- Email Management Procedure
- Business Continuity and Disaster Recovery Plan
- Risk Assessment Policy
- Risk Management Policy
- Whistleblowing Policy
- AML and Fraud Prevention Policy
- Anti-Bribery and Corruption Policy
- Disciplinary and Grievance Procedure
- Student Disciplinary Procedure
- Safeguarding Policy and Prevent Policy
- Virtual Learning Environment Policy
- Accessibility Statement (Digital)
- UKVI Sponsor Compliance Procedure

27. Approval

This policy has been approved by the Academic Board of EDA College. It forms part of the College's suite of governance and information management documents and will be communicated to all staff at induction and through the staff intranet. Students will be made aware of the relevant elements through enrolment, the VLE and the Student Handbook.

Appendix A – Minimum Technical Controls Summary

The following table summarises the minimum technical controls expected across the College's information systems. Where a system cannot meet a minimum control, the deviation must be documented, risk-assessed and authorised by the CISO with compensating controls in place.

Control Area	Minimum Standard
Identity and Access	Unique accounts; MFA for all remote, administrative and email access; least privilege; quarterly privileged access review; six-monthly access reviews for CONFIDENTIAL/RESTRICTED systems.
Authentication	NCSC-aligned password/passphrase rules; MFA via authenticator app, hardware key or equivalent; conditional access policies; banned-password screening.
Endpoint Security	Centrally managed EDR/anti-malware; full-disk encryption; supported OS; patching of critical/high vulnerabilities within 14 days; host firewall enabled; removable media controls.
Server / Cloud Security	Hardened baselines; least-privilege service accounts; logging to SIEM; vulnerability scanning at least quarterly; cloud security posture management; tenant configuration baseline reviews.
Network Security	Default-deny firewalls; network segmentation; secure remote access with MFA; protective DNS; SPF/DKIM/DMARC on all sending domains; WPA3 (or WPA2-Enterprise minimum) on Wi-Fi.
Email and Web	Anti-phishing, anti-malware and anti-impersonation controls; URL rewriting; attachment sandboxing; external sender banners; web filtering.
Data Protection	Classification and labelling; encryption in transit and at rest for CONFIDENTIAL/RESTRICTED; DLP for high-risk data flows; secure file transfer; DPIAs for high-risk processing.
Backup and Recovery	3-2-1 strategy; encrypted, immutable or isolated copies; tested restoration; documented RTO/RPO for critical systems; annual cyber-scenario exercise.
Logging and Monitoring	Centralised log collection; minimum 12-month retention; tuned detection use cases; threat intelligence feeds; 24/7 monitoring or contracted equivalent for critical services.
Incident Management	Documented Incident Response Plan; on-call arrangements; escalation to SLT/Board; ICO 72-hour notification process; OfS reportable events triage; lessons-learned process.
Supplier Security	Documented assurance for all CONFIDENTIAL/RESTRICTED processors; Article 28 terms; Cyber Essentials or equivalent for relevant suppliers; international transfer safeguards.
Training and Awareness	Mandatory induction and annual refresher training; role-based training for IT, IAOs, SLT, Board; phishing simulation programme; targeted training following incidents.

End of Policy