Riverside College
Widnes & Runcorn

IT Security Policy

Introduction

This document sets out the measures to be taken by all employees of Riverside College (the "College") and by the College as a whole in order to protect the College's computer systems, devices, infrastructure, computing environment, and any other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

Key Principles

- All IT Systems are to be protected against unauthorised access.
- All IT Systems are to be used only in compliance with relevant College policies.
- All employees of the College and all third parties, including students authorised to use the IT Systems, must ensure that they are familiar with this policy and must adhere to and comply with it at all times.
- All line managers must ensure that all Users under their control and direction adhere to and comply with this policy at all times.
- All data stored on IT Systems must be managed securely in compliance with all relevant parts of the Data Protection Legislation.
- All data stored on IT Systems must be classified appropriately (including personal data, sensitive personal data, and confidential information) with reference to Azure Information Protection Labels. All classified data must be handled appropriately in accordance with its classification.
- All data stored on IT Systems shall be available only to those Users with a legitimate need for access.
- All data stored on IT Systems shall be protected against unauthorised access and/or processing.
- All data stored on IT Systems shall be protected against loss and/or corruption.
- All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Technical Support (the "IT Department") or by authorised third parties.
- The responsibility for the security and integrity of all IT Systems and the data stored thereon lies with the IT Department unless expressly stated otherwise.
- All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and investigated by the IT Department. Any breach involving personal data shall be reported to the Data Protection Officer.
- All Users must report any security concerns relating to the IT Systems or the data stored thereon immediately to the IT Department. If concerns relate to personal data, they must also be reported to the Data Protection Officer.

IT Department Responsibilities

The Head of IT shall be responsible for:

- Ensuring that all IT Systems are assessed and deemed suitable for

compliance with the College's security requirements.

- Ensuring that IT security standards within the College are effectively implemented and regularly reviewed, working with the senior management team and Data Protection Officer, and reporting review outcomes to senior management.
- Ensuring that all Users are kept aware of the requirements of this policy and all related legislation, including the Data Protection Legislation, Computer Misuse Act 1990 and UK GDPR.

The IT Staff shall be responsible for:

- Assisting all Users in understanding and complying with this policy.
- Providing Users with appropriate support and training in IT security matters and the use of IT Systems.
- Ensuring that all Users are granted access levels appropriate for their job roles and responsibilities.
- Receiving and handling reports related to IT security matters and taking appropriate action, including informing the Data Protection Officer if personal data is involved.
- Taking proactive action to establish and implement IT security procedures and raise User awareness.
- Monitoring IT security within the College and taking necessary actions to implement this policy.
- Ensuring that regular backups are taken of all data stored within the IT Systems at least daily and stored securely both onsite and offsite. All backups should be encrypted using 256 Bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode compliant with SHA-3.

Users' Responsibilities

- Users must comply with all relevant parts of this policy at all times when using IT Systems.
- Users must only use the IT Systems within the bounds of UK law and not for any unlawful activities.
- Users must immediately inform the IT Department of any security concerns.
- Users must report any technical problems, such as hardware failures or software errors, to the IT Department.
- Any deliberate or negligent breaches of this policy will be handled under the College's disciplinary procedures.

Software Security Measures

- All software in use on the IT Systems, including operating systems, applications, and firmware, will be kept up to date with necessary updates, patches, and fixes.
- Any identified security flaws must be remedied immediately or the software removed until a resolution is available.
- No Users may install their own software without approval from the Head of IT.
- All software must be installed by the IT Department unless written permission is granted.

Anti-Virus Security Measures

- All IT Systems will be protected with suitable anti-virus, firewall, and internet security software, kept up to date with the latest definitions.

- Systems protected by anti-virus software will be subject to daily full scans.
- Any physical media used for transferring files must be virus-scanned before transfer.
- Files downloaded from cloud storage systems must be scanned for viruses.
- Any detected virus must be reported to the IT Department, even if automatically resolved.

Hardware Security Measures

- IT Systems will be located in secure, locked rooms when not in use.
- Only authorised personnel may access secured areas.
- Desktop computers and workstations must be physically secured where possible.
- Mobile devices provided by the College should be transported securely.
- The IT Department will maintain an asset register of all IT Systems.

Access Security

- Access privileges shall be determined based on job roles and responsibilities.
- All IT Systems will be password-protected with strong security policies in place and adhere to Password Policy stipulations.
- Users must not share their passwords.
- Mobile devices must automatically lock after a set period of inactivity.
- Unauthorised software that allows remote access is prohibited without approval.
- Passwords for home routers and WiFi that are used to connect to College Systems must also comply with the College Password Policy

Additional Security Measures

Cybersecurity Awareness & Training

- Mandatory annual cybersecurity training for all staff and students.
- Regular phishing simulations and awareness campaigns.
- Guidance on password hygiene, social engineering, and secure browsing.

Incident Response Plan (IRP)

- Defined roles and escalation procedures for IT incidents within the Inside Response Plan.
- Incident response aligned with National Cyber Security Centre (NCSC) guidelines.
- Semi-annual incident response drills to test readiness.

Third-Party Vendor Security

- Vendor risk assessments before engagement.
- Compliance with College security policies by all vendors handling data.
- Periodic audits of third-party data handling practices.

Cloud Security Policies

- Clear guidelines on the use of cloud services such as Microsoft 365 and Azure.
- Restrictions on unauthorised cloud storage and file-sharing services.
- Multi-factor authentication (MFA) required for all cloud-based systems.

Penetration Testing & Vulnerability Management

- Regular penetration testing of College systems.
- Scheduled vulnerability scans to identify and remediate risks.

- Compliance with Cyber Essentials certification.

Data Retention and Disposal

- Defined retention periods for different types of data.
- Secure deletion and disposal of electronic and physical data.

AI Governance and Approval

- All AI tools and services must be **reviewed and approved** by the IT Department before use within the College environment.
- Users must ensure that AI applications comply with **UK GDPR**, the **Data Protection Act 2018**, and the College's existing data protection policies.
- AI tools should only be used for educational and administrative purposes in accordance with the College's strategic objectives and policies.
- Any AI-generated content used for official purposes must be reviewed and approved for accuracy and compliance.

Acceptable Use of AI

- Staff and students may only use AI tools in accordance with the College's **IT Acceptable Use Policy.**
- Users are **strictly prohibited** from inputting personal, confidential, or sensitive College data into AI systems without prior approval from the IT Department.
- AI-generated content **must not** be used for academic dishonesty, plagiarism, or any activity that violates intellectual property laws.
- Prohibited uses of AI include but are not limited to:
    - Generating misinformation, deepfakes, or unethical content.
    - Engaging in unauthorised automated decision-making that impacts students or staff.
    - Using AI in ways that could damage the College's reputation.

Security and Data Privacy Considerations

- Users must be aware that AI tools may store and process data externally; therefore, proper **data minimization** and anonymization must be applied when necessary.
- The College will maintain an inventory of approved AI systems and assess their compliance with **privacy and security requirements.**
- Third-party AI service providers must sign **data processing agreements** ensuring compliance with the College's security standards.
- Any data breaches or security incidents related to AI tools must be reported immediately to the IT Department and the Data Protection Officer.

AI Risk Management and Monitoring

- Regular **risk assessments** will be conducted to evaluate the ethical implications, security vulnerabilities, and compliance of AI systems.
- The IT Department will monitor AI usage to ensure it aligns with College policies and does not introduce cybersecurity risks.
- Training and awareness programs will be provided to staff and students on the responsible use of AI, including identifying bias and misinformation in AI-generated content.
- Automated decision-making systems utilizing AI must have **human oversight**, with clear documentation and accountability mechanisms in place.

Related Policies

- Password Policy
- Incident Response Plan

- ICT Acceptable use Policy
- Data Breach Policy
- Data Protection Policy

Policy Review

The College shall review this policy at least once every 12 months to ensure it remains up-to-date and effective. Feedback regarding this policy should be communicated to the Head of IT and/or the Data Protection Officer.

Implementation of Policy

This policy is effective as of January 2025.