IT Policy

Document Control

The purpose of this IT Policy Document is to define, record and maintain West Herts College Group IT policies required to support the College Strategic aims and objectives. This document covers policies for:

- Acceptable Use of College Systems and Electronic Devices
- Bring Your Own Device (BYOD)
- Identity and Access Management
- Cyber Security
- Social Media
- Patch Management Policy
- Phishing Simulation

Title	IT Policy
Version	1.3
Document Author	Paul Perkins
Document Owner	Dharminder Dhanda, Director of IT and Systems
Legal Advice	None
Consultation	None
Approved By	College Leadership Group
Review Date	June 2027
Strategic Aim / Directorate	Technology
Equality Analysis	Not Required
Key Changes Made	First Issue

Purpose

Maintaining effective West Herts College Group information system policy documentation provides a sound basis for regulating how systems and procedures are designed, configured and accessed.

Scope

The policies in in this document apply to all information systems owned and used by West Herts College Group:

- Being used for College Business
- Connected to networks managed by West Herts College Group

The policies in this document apply to:

- West Herts College Group staff

- West Herts College Group students
- West Herts College Group Governors and Board Members
- Contractors, Consultants, Partners and Suppliers

Acceptable Use of College Systems and Electronic Devices

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy towards ensuring that electronic devices are used appropriately in accordance with relevant legislation and other West Herts College Group policies and procedures.

1.2 Electronic Devices include PC's, laptops, smartphones, tablets, thin client terminals, etc. used in carrying out business related activities.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members, using electronic devices PROVIDED BY THE WEST HERTS COLLEGE GROUP.

1.5 Electronic Devices are to be used in a manner that complies with the following pieces of legislation:

- Sexual Offences Act 2003;
- The Copyright and Related Regulations Act 2003;
- Computer Misuse Act 1990;
- The General Data Protection Regulation 2018
- The Road Vehicles (Construction and Use) Amendment No.4, Regulations Act 2003.

2.0 Policy Statement

General usage of devices

2.1 For students, any use associated with their programme of study or course of study for which a student is registered;

For staff, electronic devices are provided, primarily, for business use. An amount of personal use is acceptable, but should not interfere with a colleague's ability to perform their employment duties (i.e. due to volume, frequency, time expended or time of day used).

2.2 Staff' personal devices are covered under the Bring Your Own Device (BYOD) Policy, refer to the West Herts College Group BYOD policy

2.3 Electronic devices must not be used in a manner that could be deemed offensive, disturbing or upsetting. Examples of these types of activities are:

- to access and/or distribute profanity, nudity or pornography;
- to access, download or copy racist, sexist or homophobic material;
- the creation and distribution of viruses or other malware;
- to gamble
- activities that are illegal or criminally liable, either for the individual or for the West Herts College Group;
- actions that are likely to damage the West Herts College Group or its brand \ reputation; or
- distribution of copyrighted information without appropriate permission and/or approval in accordance with the Copyright and Related Regulations Act 2003.

2.4 It is the responsibility of all West Herts College Group staff, students, agency and contract workers to ensure that they have read and understood this Policy. All managers should ensure that members of their team are made aware of the Policy.

2.5 Restrictions for international usage and access to premium services for electronic devices will be set as default. Access to these facilities will only

be provided on an individual basis when a Service Desk call has been logged and where a business need is demonstrated.

2.6 Any instances where usage may be deemed inappropriate will be investigated in line with the West Herts College Group's Disciplinary Policy where appropriate.

Use of Electronic Devices whilst driving

2.7 It is illegal to drive using hand-held phones or similar devices (the rules are the same if an individual is stopped at a traffic light or queuing in traffic). Use of a hand-held mobile phone in your vehicle is permitted if:

- there is a need to call 999 or 112 in an emergency and it's unsafe or impractical to stop; and
- you are safely parked with the vehicle's engine switched off

Security of electronic devices

2.8 Electronic devices should not be left unattended. Unattended devices allow for the potential that data maybe made accessed by unauthorised individuals and may lead to an infringement of the General Data Protection Regulation.

2.9 Whilst in transport laptops and other mobile devices should be locked out of sight in the boot of a car. Equipment must not be left on desks overnight or in vehicles overnight.

2.10 Where possible, especially for staff performing business critical tasks, devices should be taken home to facilitate working from home at the time of a business continuity incident or inclement weather.

Responsibilities when using electronic devices

2.11 Staff and students are responsible for all use of electronic devices allocated to them. Therefore devices should not be used by anyone other than the individual the device is officially allocated to.

2.12 The cost of providing mobile devices is significant. Devices should be taken care of and any loss or damage should be reported to the IT Team and the colleague's line manager as soon as possible after the loss or damage.

2.13 If the device is stolen then this should be reported to the Police at the earliest opportunity and the crime number should be recorded.

2.14 With any instances of damage or loss as a result of negligence, Schools could be required to cover the full cost of replacement of the device from the nominated West Herts College Group supplier. The replacement of the device will be arranged via the IT team.

Monitoring of electronic devices

2.15 The West Herts College Group systems automatically monitor the content and volume of internet, email and network traffic from electronic devices. Systems will automatically notify IT of instances where content or volume is deemed to be inappropriate, as outlined in this Policy.

Unauthorised software

3.0 Software that has not been approved by the business is forbidden to be installed on the device this includes any virtual software to host additional Operating systems, including web browser extensions and video conferencing software.

The Electronic device will be issued with software to enable productivity for all requirements of work, projects and tasks within the organisation.

3.1 Any attempt to reimage the device, clone or jailbreak may result in disciplinary action.

4.0 Monitor and Review

4.1 This Policy will be monitored by the Director of Information Technology and Systems and reviewed annually

5.0 Associated Documents, Policies and Procedures

5.1 Documents, policies and procedures associated with this policy are:

- Disciplinary Policy

END

Bring Your Own Device (BYOD)

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy towards staff and students using personal devices (BYOD) to access College systems and data.

1.2 Bring Your Own Device covers laptops, tablets and mobile phones under this policy.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members, using electronic devices PROVIDED BY THEMSELVES

2.0 Policy Statement

Bring Your Own Device (BYOD)

2.1 Staff are allowed to use personal devices to access college systems but must agree to the requirements of West Herts College Group that the device must be compliant within the requirements of Cyber Essentials:

- Must be on a supported version of Operating system
- Must be within 2 weeks of the latest security updates
- No devices are to be used to access College data or systems that are cloned or jailbroken

Please check with the IT team if you are unsure

2.2 Staff must agree to install via Intune the College secure folder:

- This folder must be protected by Microsoft Defender
- This folder can be managed (and deleted) by the IT team via Intune
- Staff must not attempt to take College data outside this folder into personal areas on the device

- Staff must set a minimum 6 digit password on their device, it is acceptable to use biometric security, but this must be backed up by a minimum 6 digit password.

2.3 Student devices are out of scope of West Herts College Group Cyber Essentials Accreditation and are allowed for students studies, but they must not be connected to West Herts College Group networks – with the exception of Guest WiFi.

2.4 It is the responsibility of all West Herts College Group staff, students, agency and contract workers to ensure that they have read and understood this Policy. All managers should ensure that members of their team are made aware of the Policy.

Use of Software

3.0 Only software installed via the InTune folder can be used to access College data and systems.

- Only the Outlook App installed in this folder is to be used to access Email

4.0 Monitor and Review

4.1 This Policy will be monitored by the Director of Information Technology and Systems and reviewed annually

5.0 Associated Documents, Policies and Procedures

5.1 Documents, policies and procedures associated with this policy are:

- Disciplinary Policy

END

Identity and Access Management

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy towards staff and students Identity and Access Management on electronic devices used to access College systems and data.

1.2 Applies to: West Herts College Group

1.3 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members, using electronic devices PROVIDED BY WEST HERTS COLLEGE GROUP **OR** THEMSELVES

2.0 Policy Statement

Identity and Access Management

2.1 Accounts:

- Sharing of account login is not allowed, you must not share your password with anyone.
- you should protect your account by locking or logging off your computer when moving away from it.
- You must not let anyone stand over your shoulder and watch you enter your password.

2.2 Passwords and Encryption:

- Where Single Sign On isn't available you should use different passwords for each system
- For mobile devices, a 6-digit password is required
- National Cyber Security Centre recommends the use of three unrelated words, for example LampCrayonBike for nonmobile devices – West Herts College Recommend three unrelated words,

at least 14 characters, with a capital letter, a number and a special character, so in the above example it may be LampCrayonBike,2

- West Herts College current password policy follows NCSE and Cyber Essentials guidelines, so users are no longer forced to change passwords on a regular basis, due to the above password complexity being enforced.
- You may be asked to change your password periodically, West Herts College Group will use Azure password protection, so you will not be able to use passwords such as ‘password’ and you cannot increment a number at the end of your password
- All College Cloud based systems use a Multi Factor Authentication (MFA) method of securing access
- Third party access requests must be made via Service Desk and be accompanied by a business case. Access will be granted on a minimum privilege basis and within the requirements set by Cyber Essentials. IT will routinely monitor access and may revoke access if abnormal patterns spotted or rules not observed.

4.0 Monitor and Review

4.1 This Policy will be monitored by the Director of Information Technology and Systems and reviewed annually

5.0 Associated Documents, Policies and Procedures

5.1 Documents, policies and procedures associated with this policy are:

- Disciplinary Policy

END

Cyber Security

1.0 Purpose and Aims

1.1 West Herts College Group relies on its IT infrastructure to support college objectives. Information stored and processed by IT systems is a critical asset to the college. As the use of technology within businesses becomes more pervasive, the protection of the infrastructure and technologies deployed by businesses becomes more critical. Cyber Security is the protection of information processing technology (IT) systems against the threat of unauthorised or unintentional disclosure, modification or destruction of information stored and processed by IT systems.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members, accessing College systems and data, using electronic devices PROVIDED BY WEST HERTS COLLEGE GROUP **OR** THEMSELVES

1.5 Electronic Devices are to be used in a manner that complies with the following pieces of legislation:

- The Data Protection Act 1998;
- The Computer Misuse Act 1990;
- The Copyright and Related Regulations Act 2003.

2.0 Scope

2.1 This Policy applies to all IT infrastructure components under the direct management of West Herts College Group IT department including, but not limited to:

- Mobile Devices (smartphones, tablets, laptops)
- Desktop PCs
- Servers
- Virtualised systems (Hypervisors)
- Network Infrastructure Devices (Routers, switches, Wireless Access, firewalls, Intrusion Detection)
- Printers, scanners, faxes
- Memory storage devices (USB Drives, portable hard drives, DVD R/W)
- Operating Systems
- Firmware
- Business Applications
- Cloud services PaaS, IaaS, SaaS

Key Principles

2.2 West Herts College Group will achieve and maintain Cyber Essentials Accreditation.
The installation, management and configuration of IT systems is the sole responsibility of IT staff (and contractors or suppliers where required). Staff and Students outside the IT department are not permitted to install software, change settings, or attempt to access any IT systems not directly related to their role. If in doubt, individuals should consult the IT department for advice.

Security Controls

2.3 IT staff will implement controls in the following areas to reduce cyber risk throughout West Herts College Group in line with the requirements set under Cyber Essentials:

- Asset management, Maintaining an up-to-date inventory of all IT assets:

Asset Management (Hardware and Software)

2.3.1 Maintaining an up-to-date inventory of all IT assets
Updating organisation units within Active directory removing unused accounts and devices
Ensuring that the Configuration Management Database (Hornbill) is up-to-date and maintain with only active devices.
Device naming convention is strictly assigned by the device asset tag and must be removed from any database if lost, destroyed, or returned to the manufacturer.

Access control

2.4 Data and network drives

- IT staff will manage access to IT systems through a defined user access rights process which will provide, maintain and manage access to systems and information required to perform activities in support of West Herts College Group; A need to know basis is applied.
- IT staff will deploy and manage controls at the boundaries of the West Herts College Group's network infrastructure to control inbound and outbound access to/from the Colleges IT systems.
- Least privilege will be assigned to all users unless a change request has been submitted by the Head of School and authorised by the Director of IT and Systems.

Physical access

- Employees are responsible for their assigned ID access card and must immediately inform their manager at the first instance a card has been lost or stolen.
- Tailgating is forbidden when accessing an entry requiring an access card.

- Shoulder surfing is forbidden to retain any information from an employee's device, any devices monitors that require privacy will be issued privacy screen or similar.
- Under no circumstances should an employee access card be shared with any other employee or handed to contractor; contractors should be assigned a separate access card from reception when on site.
- Access to restricted areas are forbidden such as HR office, Server rooms and Principality. Anyone who does not have permission to these areas and requires access must be accompanied by authorised personnel.
- Security codes and keys are not allowed to be accessed by any unauthorised personnel.

Updates and patches

2.5 West Herts College Group will manage the configuration of all IT systems to ensure systems are configured to a consistent security baseline standard in accordance with Cyber Essentials requirements.

Updates and patches
West Herts College Group will apply security and critical updates and patches within the 14-day window of release from manufacture release.

Updates will be applied automatically; users will have the opportunity to postpone an update twice, but the third attempt will be forced and may result in the device shutting down.

Protection of Data

2.6 Protect potentially sensitive data using encryption where data is stored or transmitted.

Detection and response

2.7 West Herts College group will commission and conduct scheduled vulnerability assessments and security tests to ensure that any threats to the College network infrastructure are identified and assessed, including:

- Manage and maintain systems to detect and isolate incidents of unauthorised software (including malicious software – malware);
- Monitor, assess and respond to vulnerability alerts identified by vendors, threat news feeds and industry security alerts and ensure all IT systems are updated as recommended
- Develop and maintain a system's monitoring plan to ensure all relevant security related events are captured and assessed;

Cloud services

2.8 Where West Herts College Group consume 'Cloud Services' (IT services delivered by a third-party provider – normally through an internet connection), IT staff will develop and maintain processes to gain assurance that the College infrastructure and data cannot be compromised by a third party (i.e. service provider, customer, government agency).

- Cloud access must use Multi Factor Authentication (MFA) when accessing cloud services such as office 365
- Infrastructure as a Service (IaaS) accounts in the cloud must only be granted access by assigned administrator accounts.

Cyber security Awareness training

2.9 West Herts College Group is committed to ensuring staff and students receive appropriate cyber security training and will develop and maintain a cyber security education and awareness program.

All Staff must engage with cyber security training and with regular security tests such as Phishing emails which will involve constant monitoring that may provide additional training if required.

Cyber security awareness refresher training will be provided at regular intervals and as deemed necessary by West Herts College Group to remain current with latest cyber threats and trends.

Monitoring and reporting of IT systems

2.10 West Herts College Group monitor IT system use, including internet and email usage, for breaches of the College policies or illegal activity, including

- copyright infringement. Improper use of IT systems is a disciplinary matter.
- Attempting to download and use Illegal, copied or unlicensed software.
- Using College IT systems to access the dark web, unsecured websites and any personal cloud or network infrastructures.

3.0 Performance Measures

3.1 Cyber security within West Herts College Group with adhere to Compliance guidelines as set by the Cyber Essential scheme by the U.K Government National Cyber security Centre and will be reviewed every 12 months from initial Audit.

4.0 Monitor and Review

4.1 This Policy will be reviewed every 12 months by the Director of IT and Systems. Where review is necessary due to legislative change, changes or additions to relate to West Herts College Group policies, changes to business operations or external circumstances (significant increases in 'Cyber Threat; levels), the review will occur prior to the scheduled review date.

5.0 Associated Documents, Policies and Procedures

5.1
- The Data Protection Act 1998;
- The Computer Misuse Act 1990;
- The Copyright and Related Regulations Act 2003.
- West Herts College Group Acceptable Use Policy

END

Social Media

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy towards social media use in accordance with relevant legislation and other West Herts College Group policies and procedures.

1.2 Social media meaning any form of websites and applications that enable users to create and share content or to participate in social networking.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members.

1.5 Social media legal considerations:
- The human rights act 1998
- The General Data Protection act 2018
- The regulation of investigatory act 2000

2.0 Policy Statement

General usage of social media

2.1 Social media may only be used for business purposes by using official business social media accounts.

2.2 Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

2.3 Business social media accounts shall be protected by strong passwords in-line with the Password Policy.

2.4 social media will not be used to promote bullying, personal views, racism, hate, sharing of company data or plans.

2.5 Any communication to West Herts College Group on social media should be done with professionalism and staff or Students should not be participating in any discussion that can harm the West Herts College Group reputation. Any posts, blogs, images or text that are discovered on social media that are causing offence to West Herts College Group and its Staff or Students must be reported asap and dealt with accordingly.

2.6 Any instances where usage may be deemed inappropriate will be investigated in line with the West Herts College Group Disciplinary Policy and Managing Student Behaviour Policy where appropriate.

2.7 Responsibilities of using social media:

Social media accounts associated with West Herts College Group will only be assigned to employees that are required for marketing and promotional purposes. Social media accounts using the West Herts College Group name, brand, or visual identity can only be authorised for use by the Associate Director of Marketing & Recruitment or Director of Student Experience.

2.8 With exception of LinkedIn it is advised against associating any other personal social media accounts to West Herts College Group, as this could be used to digital footprint the College and could potentially be used to target individuals for online attacks, social engineering, email phishing, spear phishing or other cyber-attack.

2.9 Social Media Reporting:

Any topics, blogs, images, videos that are discovered online targeting the West Herts College Group in negative and inflammatory content including any offence such as Hate or bullying to Staff or Students must be reported so the correct procedures can be applied.

2.10 Social media use may be monitored via West Herts College Group firewalls which will block suspicious activity and provide alerts to any unauthorised use, which will be reported to Heads of Schools, managers and Directors.

3.0 Monitor and Review

3.1 This Policy will be monitored by the Director of IT and Systems and reviewed annually

4.0 Associated Documents, Policies and Procedures

4.1 Documents, policies and procedures associated with this policy are:

- Disciplinary Policy

END

Patch Management

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy towards Patch Management in accordance with Cyber Essentials and West Herts College Group policies and procedures.

1.2 Patch Management means software and firmware patching of network infrastructure and end user devices.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members.

2.0 Policy Statement

2.1 West Herts College Group maintain Cyber Essentials standards, so will adhere to the patching standards laid out in the Cyber Essentials current question set.

2.2 Patch management will be an ITIL process and will be controlled under ITIL standards.

2.3 All software and hardware must be kept up to date with the latest security patches.

2.4 Security patches for all software and hardware must be applied within 14 days of their release, as required by Cyber Essentials.

2.5 Emergency patches for critical vulnerabilities should be applied as soon as possible, ideally within 48 hours of release.

3.0 Responsibilities

3.1 Technical Services IT Operations is responsible for applying patches related to the infrastructure, including servers, network equipment, and phone systems.

3.2 Technical Services Delivery Team is tasked with applying patches related to end-user devices such as laptops and workstations.

3.3 Individual users are responsible for ensuring their devices are updated in line with this policy, especially for personal devices used for work purposes.

4.0 Inventory and Asset Management

4.1 A comprehensive inventory of all hardware and software will be maintained in Configuration Management Database (CMDB).

4.2 The inventory will be regularly reviewed to ensure all assets are under active support and capable of receiving necessary updates.

4.3 Data accuracy and completeness in the asset inventory must be ensured at all times.

5.0 Patch Severity and Priority

5.1 Patch severity and priority will be defined clearly and concisely, in close alignment with system criticality, vulnerability scanning, and penetration testing reports.

5.2 Patches will be classified as follows:

Critical Patches: Must be applied within 48 hours.
High Patches: Must be applied within 1 week.
Medium Patches: Must be applied within 1 month.
Low Patches: Applied as determined by the IT department.

6.0 Testing and Evaluation

6.1 Prior to widespread deployment, all patches will undergo testing in a controlled environment to ensure compatibility and mitigate potential adverse impacts on the College systems.

6.2 The processes for testing patches include verifying functionality, ensuring system compatibility, and identifying any potential conflicts.

7.0 Continuous Vulnerability Management

7.1 Continuous vulnerability scanning and penetration testing exercises will be undertaken to ensure that all weaknesses and vulnerabilities are adequately patched.

7.2 Vulnerability scanning and testing results will inform the patch management process and prioritisation of patches.

8.0 Documentation and Record Keeping

8.1 Records of all patches applied, along with dates and details of the patch will be maintained in CMDB.

8.2 Documentation of any exceptions or delays in patching must be recorded with justifications and planned remediation dates.

9.0 Change Management Records with ITSM and CMDB

9.1 IT Service Management (ITSM) tools will be utilised to record and manage the patching process.

9.2 All patch-related changes will be logged in the CMDB, including impact analysis and rollback plans.

10.0 Compliance Monitoring

10.1 Regular audits will be conducted to ensure adherence to this policy.

10.2 Non-compliance must be addressed immediately, with corrective actions documented and implemented.

11.0 Training and Awareness

11.1 All members of Technical Services will receive regular training on the importance of software updates and this patching policy.

11.2 Awareness campaigns will be conducted to keep the importance of patch management in focus.

12.0 Incident Response

12.1 In the event of a security incident related to unpatched systems, an incident response will be initiated in accordance with the West Herts College Group Incident Response Plan.

13.0 Review and Update

13.1 This Policy will be monitored by the Director of IT and Systems and reviewed annually or following significant changes to IT infrastructure or cybersecurity threats.

14.0 Exceptions

14.1 Any exceptions to this policy must be approved by the Director of IT and Systems and documented with a review date.

15.0 Associated Documents, Policies and Procedures

15.1 Documents, policies and procedures associated with this policy are:
• Disciplinary Policy

END

Phishing Simulation

1.0 Purpose and Aims

1.1 This policy establishes the guidelines for conducting regular phishing simulation exercises within the West Herts College Group.

1.2 The primary objective of these simulations is to enhance the awareness and preparedness of our staff against phishing attacks, thereby strengthening our overall cybersecurity posture.

1.3 Applies to: West Herts College Group

1.4 This policy applies to all West Herts College Group staff, Students, agency or contract workers, volunteers and Board or Committee members.

2.0 Objectives

2.1 To assess and improve the ability of staff to identify and respond to phishing attempts.

2.2 To ensure staff are familiar with the organisation's procedures for reporting phishing attempts.

2.3 To measure the effectiveness of current cybersecurity training and identify areas for improvement.

3.0 Responsibilities

3.1 The IT Operations team:

- Oversee the setup and delivery of phishing simulations, ensuring seamless operation.

3.2 Cyber Security Officer:

- Analyse each phishing simulation's effectiveness, assessing employee responses and identifying key trends.
- Generate concise reports summarising campaign outcomes, vulnerabilities, and engagement, along with targeted recommendations for future campaigns.
- Suggest updates to cybersecurity policies and training programs based on campaign insights to strengthen organizational security awareness.

3.3 All Employees:

- To actively participate in simulations and follow reporting procedures for suspected phishing attempts.

4.0 Simulation Frequency

4.1 Phishing simulations will be conducted quarterly to ensure continuous learning and adaptation to evolving phishing tactics.

5.0 Conduct Guidelines

5.1 Simulations will be designed to mimic real-life phishing scenarios without causing undue alarm or disruption to work.

5.2 The IT Operations team, in collaboration with the Cyber Security Officer will oversee the design, execution, and review of phishing simulations.

6.0 Reporting and Feedback

6.1 Employees who identify a phishing email should report it to the IT Helpdesk.

6.2 Immediate feedback will be provided to participants who interact with the simulation, with educational resources to help them recognise future phishing attempts.

7.0 Non-Punitive Environment

7.1 The focus of the phishing simulation exercises is educational, not punitive. The objective is to learn and improve, not to reprimand.

8.0 Data Analysis and Reporting

8.1 Cyber Security Officer will analyse the results of each campaign, providing detailed reports on engagement, areas of vulnerability, and recommendations for further training.

9.0 Continuous Improvement

9.1 The cybersecurity training program, including phishing simulations, will be regularly reviewed and updated based on the outcomes of simulations and evolving cyber threats.

10.0 Policy Review and Amendment

10.1 This policy will be reviewed annually or following significant changes to our operational environment or cybersecurity landscape. Amendments will be made as necessary to ensure the continued effectiveness of our phishing simulation exercises.

11.0 Exceptions

11.1 Any exceptions to this policy must be approved by the Director of IT and Systems and documented with a review date.

12.0 Associated Documents, Policies and Procedures

12.1 Documents, policies and procedures associated with this policy are:

- Disciplinary Policy

IT Procurement

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy regarding the procurement of IT systems and services to ensure cost-effective, secure, sustainable, and compliant technology acquisitions.

1.2 Applies to: West Herts College Group

1.3 This policy applies to all West Herts College Group staff, students, agency workers, and contract staff involved in IT procurement across the college.

2.0 Policy Statement

2.1 The college's IT procurement activities are guided by the following principles and practices:

3.0 Objectives

3.1 Support the educational and operational needs of the college through efficient procurement processes.
3.2 Ensure transparency, fairness, and accountability throughout vendor selection.
3.3 Maintain compliance with legal, financial, security, and framework regulations.
3.4 Optimise value for money while mitigating procurement-related risks.

4.0 Roles and Responsibilities

4.1 IT & Systems Team: Identify requirements, evaluate solutions, and support technical assessments.

4.2 Procurement Officer: Coordinate procurement activities, ensure compliance, and manage supplier relationships.

4.3 Finance Department: Review budget feasibility and approve expenditure.

4.4 IT Senior Leadership Team: Provide final approval for strategic IT purchases.

5.0 Contract Management

5.1 Contracts must include clear service agreements, defined support levels, warranties, and SLAs.
5.2 Vendors will be reviewed regularly to evaluate performance and ensure compliance with contractual obligations.
5.3 A documented process for dispute resolution and corrective actions will be followed if service expectations are not met.

6.0 Compliance & Security

6.1 All vendors must comply with relevant data protection regulations, including GDPR.

6.2 IT assets must align with current cybersecurity best practices.

6.3 The college prioritises ethical, sustainable, and inclusive procurement.

6.4 Preference will be given to eco-conscious technologies, such as energy-efficient equipment and responsible e-waste disposal.

7.0 Monitor and Review

7.1 This policy will be monitored by the IT & Systems team and reviewed annually by the IT Senior Leadership Team to ensure continued relevance, effectiveness, and compliance with regulatory standards.

8.0 Exceptions

8.1 Any exceptions to this policy must be approved by the Director of IT and Systems and documented with a review date.

END

IT Sustainability

1.0 Purpose and Aims

1.1 This document sets out the West Herts College Group policy regarding the commitment of the IT department to sustainability and environmental responsibility in all areas of its operations.
1.2 Applies to: West Herts College Group
1.3 This policy applies to all West Herts College Group staff, students, agency workers, and contract staff involved in the procurement, maintenance, and disposal of IT equipment and services.

2.0 Policy Statement

2.1 The college's IT department is committed to reducing its environmental impact and promoting sustainable practices. This includes implementing energy-efficient technologies, ensuring responsible procurement, and encouraging recycling and awareness among staff and students.

3.0 Objectives

3.1 Reduce energy consumption through efficient technologies and operational practices.
3.2 Promote recycling and the responsible disposal of electronic waste.
3.3 Ensure environmentally responsible procurement aligned with supplier sustainability credentials.
3.4 Raise environmental awareness among the college community.
3.5 Monitor and assess the IT department's environmental performance regularly.

4.0 Roles and Responsibilities

4.1 IT & Systems Team: Implement sustainable technologies, conduct audits, and monitor environmental performance.
4.2 Procurement Officer: Source environmentally responsible products and suppliers.
4.3 Facilities & Estates: Collaborate with IT in e-waste collection, recycling, and sustainable disposal.
4.4 IT Senior Leadership Team: Oversee strategic sustainability initiatives and policy updates.

5.0 Sustainable Practices and Actions

5.1 Energy-Efficient Equipment: Prioritise purchasing low-power computers, servers, and peripherals.
5.2 Power Management: Enforce power-saving settings on all devices during periods of inactivity.

5.3 E-Waste Management: Maintain a system for the secure, ethical disposal and recycling of IT assets.

5.4 Sustainable Procurement Policy: Incorporate environmental standards into procurement processes and supplier selection.

5.5 Training and Awareness: Deliver training and resources to raise awareness and engage staff and students in sustainable practices.

5.6 Green IT Operations: Embrace green solutions such as virtualisation, cloud computing, and server consolidation.

5.7 Environmental Audits: Conduct regular reviews of IT equipment and processes to assess compliance with sustainability goals.

6.0 Compliance & Environmental Standards

6.1 All operations must comply with applicable environmental legislation and the college's sustainability strategy.

6.2 Procured IT products must support environmental best practices such as low emissions, reduced packaging, and energy efficiency certifications.

6.3 Suppliers must adhere to ethical and sustainable production and disposal methods.

7.0 Monitor and Review

7.1 This policy will be reviewed annually by the IT Senior Leadership Team to ensure alignment with evolving technologies, environmental legislation, and best practices.

8.0 Exceptions

8.1 Any exceptions to this policy must be approved by the Director of IT and Systems and must be documented along with an agreed review date.

END