

IT Security and Acceptable Use Policy

IT Security and Acceptable Use Policy

West Herts College (WHC) uses IT services for its teaching and administrative activities. The main purpose of this policy is to define how it maintains IT security and what it constitutes as acceptable use; to encourage the responsible use of facilities; to maximize the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimise the risk of misuse from inside or outside WHC.

These regulations incorporate the acceptable use policy of our service provider, JISC (Joint Information Systems Committee), which manages network connections between Colleges and the Internet (the JANET Network). The full text of their policy can be found at:

<https://community.jisc.ac.uk/library/acceptable-use-policy>

What does this Policy cover?

- The use of all IT services and facilities provided by WHC
- All devices irrespective of ownership when connected to the WHC communications network services run by Technical Services (TS) which may be used by any member of WHC staff
- Use and access of CCTV
- Access to externally hosted systems

Acceptable Use of IT Equipment

What constitutes authorised use?

- For students, any use associated with their programme of study or course for which a student is registered; and reasonable personal use
- For staff use in the course of their role and directly associated with their employment, and reasonable personal use

What does reasonable personal use mean?

Incidental and occasional use which does not:

- disrupt or distract the individual from the efficient conduct of WHC business (i.e. due to volume, frequency, time expended or time of day used)

- involve accessing, downloading, storing or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence
- restrict the use of those systems by other legitimate users
- risk bringing WHC into disrepute or placing WHC in a position of liability
- add significantly to running costs to the college
- breach the regulations set out by our internet provider Janet

Connecting and Downloading Software and Applications

- When Connecting WHC devices to the college network, users take reasonable precautions to prevent the introduction of any virus, worm, Trojan Horse or other harmful program to any computer, file or software. You should not click open emails from unknown sources and never click on links in unknown emails
- Only college equipment can be connected to the college 'WHC' network. Personal phones can be connected to the guest Wi-Fi network
- Respect the copyright of all materials and software that are made available by WHC service providers and third parties for authorised use
- Users must not make, run or use unlicensed copies of software or data. They should only download data or datasets where they are explicitly permitted to do so.
- Software licensing conditions of use must be abided
- Users should be aware that, unless otherwise stated, software and datasets provided by WHC should only be used for WHC educational purposes
- Comply with the Computer Misuse Act of August 1990 which makes activities such as hacking or the deliberate introduction of viruses and other malware a criminal offence

Passwords and Encryption

- Make sure you use different passwords for each of your accounts
- Be sure no one watches when you enter your password
- Always log off or lock your computer if you leave your device
- Do not tell anyone your password or let them use your account
- Change your passwords periodically when prompted to do so
- Use strong passwords (Staff at least 8 characters, students 8 characters)
- Use a password manager to store your passwords such as 'KeePass'. Contact 01923 81 2424 for installation
- National Cyber Security Centre advise on having 3 unrelated words for your password and can remember with a visual. "horseenjoyscinema" is easy to remember but would take long time to crack
- The College use Azure Password protection to safeguard your passwords and therefore you will not be able to use insecure words for your passwords such as "password", nor will you be able to increment the numbers on a password.

- Always use Multi Factor Authentication (MFA) for external services where possible.

How to Store Data

- Only store data on WHC shared areas, Sharepoint and One drive. Never save documents to your desktop, or computer hard drive as it is not secure and not backed up by college systems. Data stored to your C: drive and desktop will be lost in the event of a hardware fault on the drive.
- Please be aware Share Point and One Drive are not backed up by the college but have a 7 year retention policy set by Microsoft.
- Do not use, USB Sticks, external hard drives, dropbox or other cloud solutions (non O365) as when you leave the college, the data is no longer accessible by WHC staff and other forms of storage are not protected or guaranteed to be as safe as College. Also, this will not be backed up as per current WHC data backup and retention policies

Sending Emails

- Don't send passwords in emails, as they are sent using clear text (anyone can read it). Please send username by email and ring the user to confirm password. (sending an email to inform them of username and a separate email detailing password is NOT secure.)
- Don't send confidential content, names or personal information in emails. Technical Services can set up an account on a secure portal or we can send via SFTP. Please ring the Helpdesk 01923 812424 for further advice.
- If you need to share volumes or sensitive data for external companies, Technical Services can create them a login on the portal. Technical Services will give you access to place the confidential data on the U drive and the customer can login and pick the data up securely. This is also useful when trying to send large file over 30MB as most organisations set this as an upper limit for sending and receiving files.
- If you wish to share confidential data with another department, Technical Services can set up a folder on a internal shared area where documents access can be restricted to individuals or departments.

What you must not do:

- Do not share your logon with anyone as you will be liable for misuse.
- Use material or programs in a way which is unlawful, defamatory, or invasive of another's privacy
- Don't add, engage in or encourage conversations with students on social networking

sites

- Use the IT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data
- Use the IT services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party
- Jeopardize the provision of services (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources)
- Publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent or unlawful. Such materials will always include, but at the colleges discretion may not be limited to, items deemed to be offensive, discriminatory, obscene, indecent or unlawful
- Use IT facilities in a way that brings or could bring the college into disrepute. This includes associating WHC with external facilities such as Websites that could bring the college into disrepute by association
- Disclose or share credentials e.g. password to others, or use accounts or passwords belonging to others, or otherwise to circumvent registration procedures
- Access or attempt to access any data processing systems or services at college or elsewhere without permission or facilitate unauthorized access by others
- Attempt to circumvent any firewall or software designed to protect systems against harm
- Interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorized software on to any College IT facilities)
- Attempt to disrupt services. Hacking is defined here as the unauthorized access or modification of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter records, or to facilitate the commission of a crime
- Interfere with, disconnect, damage or remove without authority any equipment
- Do not click on any links in phishing emails and provide further account details. If you have done this please power off your device (by holding the power button in for 10 secs) and RING the helpdesk immediately on 01923 812424. If you ignore this advice you could be responsible for contributing to a Cyber attack on the college. **Security and IT Equipment**

Lost or Stolen Devices

What do if you lose your laptop, phone, barrier access staff card or a college device?

- It's important that all staff look after college equipment however should something be stolen/lost it is vitally important to report this to technical services as soon as possible on 01923 812424. This will ensure it is wiped, locked out and data/ information is not accessible. This is particularly important now Multi Factor Authentication (MFA) is in place

Disposal Devices

- All IT devices must be disposed of through the colleges designated electrical disposal company. The company will provide a certificate to prove safe disposal. Computing equipment returned to lease companies must provide the same certification. This is arranged through the Estates team on 01923 812366.

Monitoring of college network, systems, staff and students accounts

The college monitors its systems and networks only in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR).

Computer systems may be monitored or recorded to secure effective system operation and for other lawful practices. For example, monitoring of user accounts might occur if the college has reason to believe that its computer facilities were being misused to send unsolicited commercial e-mail.

The College reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties.

Students and staff's access to blocked/ restricted sites include:

- Sexually explicit content
- Discrimination
- Drug Abuse
- Explicit Violence
- Extremist Groups
- Illegal or Unethical activities
- Gambling
- Sports Hunting and War Games
- Weapons (Sales)
- Peer-to-peer File Sharing
- Malicious Websites
- Phishing, SPAM URLs, Digital Postcards, Proxy Avoidance

When students or staff access blocked sites there is an entry written in the firewall log. Authorised staff may, when requested by the College Leadership Group, investigate what sites students or staff have been accessing for example in the case of a criminal investigation.

Procedures for accessing staff and students accounts

On rare occasions it may be necessary to access a member of staffs account should there be significant impact on the college / students if the College didn't access it.

Accessing Accounts	
Students	Head or rel Colle Lead Grou
Staff	Direc Huma Reso Princ Princ
Visitors, Contractors, Subcontractors	Head Techn Servic

Procedures for dealing with misuse or suspected security violations

In the event of suspected misuse of IT facilities user accounts maybe suspended and be inspected, monitored, files maybe accessed where necessary. Technical Services may also disconnect network services, prevent access to the facilities without notice while investigations proceed.

Cases of misuse or abuse should be reported to:

Misuse by:	
Students	Head Scho relev Colle Lead Grou mem
Staff	Direc Huma Reso
Visitors, Contractors, Subcontractors	Head Tech Servi

Any use that falls outside of these definitions is prohibited and may lead to disciplinary procedures being invoked, with penalties that could include suspension from the use of all computing facilities for extended periods.

For Staff serious cases may lead to disciplinary action, up to and including suspension, dismissal without notice and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against the college and any legal action to which the college is, or might be, exposed as a result of your unauthorized use.

For Students cases may lead to disciplinary action, including suspension or permanent exclusion from college and evidence will be provided to the police when requested to in the event of any criminal investigation.

VPN, Portal & Home Router Protocols

All staff must access college business systems via the VPN Forticlient. Staff must change their home router default password upon installation as this will otherwise be programmed with the standard password and pose a security risk. VPN is restricted to UK access only.

Process is as follows: -

- Staff access abroad – HR must authorise access is required for a staff member
- Student access abroad – HOS must authorise VPN to be opened for individual student request confirming the request is genuine.
- Access from home to the portal via a personal device must contain an updated Virus checker, Operating system must be in support and the Software Firewall must be turned on.

Mobile Phone Policy

College provided Mobile Phone

Staff who have a college mobile phone must adhere to the following: -

- Report it immediately if lost or stolen to Helpdesk on 01923 812424 so that Technical Services can block the number
- Keep it updated as soon as IOS and Android update notifications are issued
- Ensure it is only used for college business and note web browsing is monitored as per usual college procedures
- Report any scams to the helpdesk on 01923 812424 Personal Mobile

- If you have added your college email account to your personal phone you must make sure your phone is updated as soon as IOS and Android update notifications are issued
- Your personal device must not have the “rooted” or “jailbreak” functionality

BYOD (Bring your own device)

You can use your personal device on the WHC-GUEST wi-fi. All staff must logon using their normal college credentials.

You should ensure your device has:-

- An up-to-date virus checker
- Latest windows or IOS updates
- Operating System that is in support

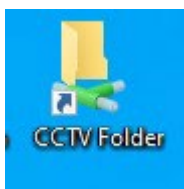
CCTV Protocols

The college does not monitor live video feeds from its CCTV it is only licenced to access it retrospectively.

If there is a requirement to access footage permission must be sort from a member of Senior Management Team or a member of the Safeguarding Team.

Footage is only to be viewed by authorised staff and not be viewed publicly. On rare occasions it may be necessary for the police to request access or copies of CCTV this should be authorised by a member of College Leadership Group or the Safeguarding team. A data request form is required when requests are made by the police.

Footage is retained for 30 days as per regulations. All footage that is viewed in connection to an incident should be downloaded to the CCTV folder on the secure shared area. Staff members with permitted access will see an icon on their desktop.



This should not be downloaded anywhere else. This provides an audit trail and ensures it is available if it is required in the future regardless of how clear or useful it is and available to all authorised users.

Authorised by	Updated
CLG (SK)	NOVEMBER 2022