Information Services & Technology

IS&T Usage Policy

Status: Definative
UCLG Approval: 10th August 2022

Writtle University College
Lordship Road, Chelmsford
Essex, CM1 3RR

Tel: +44 (0)1245 424200
Fax: +44 (0)1245 420456
Email: info@writtle.ac.uk
www.writtle.ac.uk

CONTENTS

1 OPENING STATEMENT 4

2 INTRODUCTION 5

3 POLICY SUMMARY 5

4 HARDWARE 5

4.1 PURCHASE 5
4.2 MOVEMENTS 5
4.3 REVIEW 6
4.4 DISPOSAL 6
4.5 SECURITY 6
4.6 PERSONAL EQUIPMENT (PC, LAPTOP, ETC.) 6
4.7 OTHER EQUIPMENT 7
4.7.1 Mobile Phones 7
4.7.2 Games Consoles, TVs, Virtual Assistants, etc. 7
4.7.3 Miscellaneous 7

5 SOFTWARE 7

5.1 COMPLIANCE & DOCUMENTATION 7
5.2 ACQUISITION 7
5.3 DELIVERY 8
5.4 INSTALLATION 8
5.5 ON STAFF/STUDENT OWNED PCS 8
5.6 MAINTENANCE 9
5.7 AUDIT 9

6 USE OF FACILITIES 9

7 DATA PROTECTION 10

8 NETWORK CONNECTIONS 10

9 STUDENT NETWORK CONNECTIONS 10

10 ACCOUNT MANAGEMENT 11

10.1 STAFF 11
10.2 STUDENTS 11
10.3 PRIVILEGED ACCESS 11

11 PASSWORDS 11

11.1 MULTI-FACTOR AUTHENTICATION 12
11.2 NETWORK /SYSTEM PASSWORDS 12

12 VIRUSES 12

13 STORAGE 13

13.1 STORAGE LOCATIONS 13
13.1.1 Personal User Space - N Drive (Staff & Students) 13
13.1.2 Shared Storage Space - G Drive (Staff Only) 13
13.1.3 Temporary Storage - T Drive (Staff & Students) 13
13.1.4 PC Hard Drive - C Drive (Staff Only) 14

13.1.5 One Drive 14
13.1.6 External Media (USB sticks, external hard drives, CDs) 14
14 EMAIL 15
15 INTERNET 16
16 AUDITING 16
17 PRINTING & PHOTOCOPYING 16
17.1 STAFF 16
17.2 STUDENTS 16
18 MOBILE/LAPTOP USERS 17
19 SUPPORT 17
19.1 STAFF 17
19.2 STUDENT 17
20 BACKUP AND RESTORE 18
20.1 STAFF 18
20.2 STUDENT 18
21 PATCHING 18
21.1 REMOVAL OF INSECURE SYSTEMS 18
21.2 SECURE CONFIGURATION AND PATCHING 18
21.3 MICROSOFT WINDOWS 19
21.4 NON-MICROSOFT PLATFORMS 19
21.5 BRING YOUR OWN DEVICES (BYOD) AND INTERNET OF THINGS (IOT) 19
22 **BREACHES OF THIS POLICY 20**
23 DOCUMENT CONTROL: 20

1 OPENING STATEMENT

It is the individual responsibility of all Writtle University College employees and students to fully read the 'Information Services & Technology Usage Policy'. The use of Writtle University College IT facilities indicates an agreement to be bound by the conditions of this policy. Any concerns regarding adherence to this policy should be referred to the appropriate Line Manager/Lecturer, or to the Information Services & Technology (IS&T) Manager.

The Board of Governors and Leadership Group of Writtle University College are conscious of, and acknowledge **all** computer software copyrights without exception and will strictly adhere to the Terms and Conditions of any licence to which the institution is a party.

Writtle University College will not condone the use of any software, irrespective of prevailing circumstances, that does not have a licence. Any employee, student or external user of Writtle University College provided equipment found to be using, or in possession of, unlicensed software will be the subject to disciplinary procedures or have their access rights removed as appropriate.

2 INTRODUCTION

Writtle University College (WUC) strives to provide the best possible IT provision to staff and students with the fewest possible restrictions. Each individual using the IT facilities is deemed thereby to agree that their use of the facilities will remain within the bounds of the IS&T Usage Policy and other related WUC policies.

Guidelines and procedures for the use of WUC IT facilities are published on Moodle (https://moodle.writtle.ac.uk) and MyWi (https://mywi.writtle.ac.uk).

3 POLICY SUMMARY

This Policy will be reviewed on a regular basis, normally annually.

For the purpose of this document, references to "device" inlude PCs, Laptops, Tablet, mobile phones and any other device connected to the WUC network. Some aspects of this policy also cover any device connected to the Student Network in the Halls of Residence and elsewhere, while others cover the usage of WUC services (e.g. e-mail) irrespective of where they are used.

Anyone found to be in breach of this policy will be subject to disciplinary action.

4 HARDWARE

4.1 PURCHASE

All IT related hardware* purchases must be authorised by the IS&T department to ensure that they are appropriate and will work with the existing infrastructure. New purchases must be made available to IS&T to allow an asset number to be attached and details recorded in the asset register. Where appropriate, financial asset details will also be recorded.

* - If in doubt please consult the IS&T department

4.2 MOVEMENTS

Movement of IT equipment must only be undertaken with the prior approval of IS&T in order to ensure that appropriate software can be added or removed and the asset register updated. Failing to comply will give rise to future auditing queries. Any individual found doing so will be in breach of this policy and may be subjected to disciplinary action.

Assets can only be permanently taken off campus with the approval of both the appropriate line manager and the IS&T Manager. There should be a specific reason why WUC equipment needs to be taken off campus which should be detailed with the request. When equipment leaves the campus it becomes the responsibility of the person doing so and will be recorded as such in the IS&T asset register.

Portable equipment (laptops, tablets, etc.) are recorded in the asset register as "belonging" to the current user. Should the equipment permanently change hands, IS&T must be informed to allow the asset register to be updated and responsibility transferred.

4.3 Review

IS&T carry out a rolling annual review of the asset register to ensure equipment is at the recorded location. Portable equipment will be checked against the person listed as having the equipment. It will be that person's responsibility to confirm the equipment is still in their possession and provide visual evidence if required.

4.4 Disposal

Hardware disposals may only be carried out by the IS&T department via an approved disposal contractor. This ensures that:

- All storage media (e.g. hard drives, memory sticks) are disposed of in a manner that will ensure the destruction of all data held
- Equipment is disposed of in accordance with the WEEE (Waste Electrical and Electronic Equipment) European Directive
- WUC does not breach data protection legislation

4.5 Security

Default passwords must be changed on all devices before they are connected to the WUC network infrastructure.

Physical security of hardware will largely depend upon the location in which it is installed and the access that is available to staff and students:

- **Staff Offices**: These are normally staffed or secured when empty. As such, no extra physical security is required on the devices to ensure it remains secure.
- **Student Areas**: Some devices located within student areas need to be secured with an appropriate Kensington style lock. This will ensure some degree of movement whilst securing the device.
- **Portable equipment:** Security of these items is the responsibility of the current user/holder. Their security should be reviewed each time they are used to ensure they are not liable to be stolen.
- **Server Rooms**: Server room access is restricted to IS&T staff only (with the exception of essential Property staff). This ensures that the security of the equipment within is maintained. Doors to these locations must be kept locked at all times when not in use. Contractors should not be left unattended within these rooms unless they are well known to WUC and staff are certain of their responsibilities.

Any loss of WUC equipment must be reported to the IS&T Manager for recording in the asset register and investigation into any security/data breach which may occur as a result. The user of the lost item will also need to liaise with their line manager/DPO regarding any data loss and possible implications.

4.6 Personal Equipment (PC, Laptop, etc.)

Staff who use their own equipment, either on or off the campus, must ensure that any information they use is kept secure and only for as long as is necessary. All WUC related

files must be deleted as soon as possible – and cleared from the Recycle Bin. Security of this information is the responsibility of the equipment owner and any loss or potential loss of data must be reported to their line manager as soon as the loss is noted.

Personal devices must be password protected to ensure against unauthorised access to data. Data should not be available to others that may use the personal equipment.

4.7 Other Equipment

4.7.1 Mobile Phones

IS&T will assist in enabling users to connect their mobile phones to the WUC network where necessary. It is the responsibility of the user to ensure the security of all information stored on or accessible from such devices. Information transferred/stored should be appropriate and only kept on the device for as long as it is required.

4.7.2 Games Consoles, TVs, Virtual Assistants, etc.

Students are permitted to bring network enabled devices to WUC for use in the Halls of Residence and use them within the confines of their room. Connection to the network will be may be restricted if IS&T deem appropriate. As an example, access to some online games/services may not be allowed if there is suspicion that it may allow unauthorised access to the WIC network/facilities.

4.7.3 Miscellaneous

All other types of equipment such as hubs, routers, switches, etc. must not be plugged into the WUC network without prior approval from the IS&T Manager. Use of such equipment may cause problems for other network users.

5 SOFTWARE

5.1 Compliance & Documentation

All original licensing information will be centrally managed by IS&T. Physical media will, where possible, be copied onto the network for safe storage.

5.2 Acquisition

All computer software (irrespective of prevailing Licensing conditions, for example 30 Day Evaluation, Shareware, Freeware, Academically Licensed, etc.) acquired for and on behalf of WUC must be obtained via IS&T, without exception. This is to ensure that:

- Appropriate licences are in place and lodged for safekeeping
- WUC does not already have something similar in place
- The software is compatible with existing equipment/software and is deemed fit for the purpose for which it is intended

It is expressly forbidden for an individual to purchase and pay for software for use on WUC equipment without first consulting the IS&T Department. Any individual found doing so will be in breach of this policy and will be subjected to disciplinary action.

Individuals who would like to use their own software on WUC PCs must have the prior authorisation of the IS&T department and provide appropriate evidence that this is acceptable, both in terms of the number of installations that exist and that the software is licensed for commercial use.

Any request for software should be directed in the first instance to the appropriate line manager who can then forward a request to the IS&T Manager. In the event that IS&T determines that a product should not be purchased for whatever reason, a suitable alternative to achieve the required goal will be recommended if possible.

Failure to adhere to this policy will result in the offending software being uninstalled forthwith from the WUC Network and/or standalone personal computer irrespective of type e.g. Desktop, Laptop, etc.

5.3 Delivery

All newly purchased software will be delivered to the IS&T department, where a nominated member of staff can check and verify that the WUC License Register has been suitably updated.

5.4 Installation

Only members of IS&T can install software on WUC PCs.

For the majority of software, WUC staff/students do not have the appropriate network permissions to enable them to undertake any installation. Software that does not require administrative prviledges to install must not be installed as it may adversely impact other individuals using the equipment.

Staff laptop users do have permissions and are given the authority to install software as and when required. This is primarily to allow them to connect to networks externally of WUC when off campus. They must still abide by the IS&T Usage Policy in terms of licensing. Any individual found to be in breach of this policy will be subject to disciplinary action.

5.5 On Staff/Student Owned PCs

In some cases, depending on individual licence agreements, software purchased by WUC may be legally installed on PCs owned personally by employees or students of WUC. Any such software must be removed immediately when the owner is no longer employed by, or studying at WUC.

5.6 MAINTENANCE

Software must be maintained in line with manufacturer's instructions. Any required patches (especially security patches) must be applied as soon as practicable after their release.

IS&T will be responsible for the maintenance of WUC servers / PCs and application of any necessary patches. Staff and students are responsible for the patching their personal equipment. IS&T cannot be held responsible for any damage caused to personal equipment by the installation of recommended patches.

5.7 AUDIT

The WUC IS&T department will undertake a rolling audit of all WUC owned devices to ensure that only licensed software is installed and where licensing is for a limited number of installs, the maximum number of installs has not been exceeded.

Laptop/tablet users must ensure that they make the equipment available as and when required to allow an audit to take place.

6 USE OF FACILITIES

The WUC IT systems and resources shall be only used for legitimate academic purposes, including instruction, research, administration, public information and service, limited personal use or other approved tasks. WUC IT facilities must not be used for:

- Any activity that violates the integrity or interferes with the normal operation of the WUC IT systems and network
- Unauthorised use of another person's identity and password
- Unauthorised transfer of files
- Unauthorised access to a file to use, read, change or delete its contents
- Any other activity that interferes with the work of WUC, another student, staff member, or other organisation
- Unauthorised financial gain or commercial activity
- WUC has a statutory duty, under the Counter Terrorism and Security Act 2015 (termed "PREVENT") to aid the process of preventing people being drawn into terrorism. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist.
- Unauthorised reproduction or distribution of copyrighted material including software, text, images, audio or video

WUC reserves the right to monitor usage and traffic for the following circumstances:

- if any infringement of the above are suspected
- to protect Staff and Students within the context of Safeguarding and PREVENT

Users should note that criminal proceedings could apply, which could lead to imprisonment, as some of these offences breach criminal law.

If any user believes for whatever reason that they, or another person, has access to systems, software or data that they are not authorised to access, they should report it to the IS&T Manager and their Line Manager/Lecturer immediately.

Users found to be in breach of these rules will be subject to disciplinary action that may involve the Police.

The use of personal hardware/media is at the user's risk and WUC will not be held responsible for any damage that may occur as a result. 'Personal hardware/media' includes, but is not limited to: CDs (blank/recorded), DVDs, memory cards, memory sticks and external hard drives.

7 DATA PROTECTION

All computer processing of data relating to living individuals must be registered and be undertaken in accordance with WUCs Data Protection policy. Such processing may only be carried out on designated computers owned by WUC.

More information can be found in the WUC Data Protection policy available on the Intranet - MyWi (https://mywi.writtle.ac.uk).

If data is required off campus, consider the use of the VPN to connect/access the data rather than taking data off campus. Consider:

- Connecting to the network via the Virtual Private Network (VPN)
- Accessing the information remotely via the Writtle File Access (https://wfa.writtle.ac.uk) facility to remove the transport of files between locations
- The use of password options within applications (i.e. Microsoft Office suite)

8 NETWORK CONNECTIONS

Connection to the main WUC data network is limited to approved devices such as WUC supplied PCs & laptops, staff/student PCs & laptops and other devices as approved by the IS&T Manager. Other devices must not be connected to the WUC network without prior approval from the IS&T Manager.

The terms of the JANET Acceptable Use Policy (https://jisc.ac.uk/janet) are deemed to apply to the WUC data network even where network traffic does not travel outside WUC.

9 STUDENT NETWORK CONNECTIONS

The Student Network is available in all halls of residence, the majority of teaching spaces and in various other WUC locations. All Internet access is subject to the JANET Acceptable Use Policy. Students using such connections must ensure that their devices are kept up to date and free from viruses, spyware, malware, etc. in order to avoid affecting other equipment.

10 ACCOUNT MANAGEMENT

Accounts for use by staff and students are only created by appropriate individuals.

10.1 STAFF

Creation: accounts are created by the HR department just prior to the individuals commencement of work. The default account will only have access to the user's N drive and the T drive. For additional access to the G drive, access must be requested by their line manager/data owner via email/INSERT. Access to other WUC systems (e.g. Resource, Unit-E) must be requested via the systems owner.

Closure: accounts are closed automatically based upon a closure date supplied by HR. Other manual checks/changes are undertaken before and after the individual's leaving date. The account then remains on the system for three months, before being exported (email and N drive space) and deleted. The archived data will remain available for a further nine months, after which it will be permanently deleted.

10.2 STUDENTS

Creation: accounts are created during enrolment.

Closure: closure of student accounts takes place during October when all students who are no longer studying with WUC have their accounts closed. In July, all closed accounts for students not enrolled since the end of the previous academic year (those closed the pervious October) are removed from the system. No backup of data is kept.

10.3 PRIVILEGED ACCESS

Privileged access enables an individual to take actions which affect the accounts and files of other users. Such access is granted by the IS&T Manager to staff performing system administration and other support tasks.

Individuals with privileged access must respect the privacy of other users and the integrity of the systems and data.

In particular, privileged access shall:

- only be granted to authorised individuals
- only be used to perform assigned job duties
- not be used for unauthorised viewing, modification, copying, or destruction of system or user data.

11 PASSWORDS

The WUC network is a controlled environment and all users will have a network account for access to services including, but not limited to, the PC network, e-mail and applications. Passwords (including those for separate applications) should never be divulged to a third party without good reason. Passwords must never be written down. If

there is a need to have a physical reminder of a password, write a hint or clue to the real password e.g. “my first car registration number”.

Passwords must be at least eight characters long and made up of a combination of all of the following characters:

- English uppercase characters (A - Z)
- English lowercase characters (a - z)
- Base 10 digits (0 - 9)

Try to mix all a combination of the above to create a stronger password. Consider use both upper and lower case letters and numbers to represent letters (e.g. `Fudg3C4k3` instead of `fudgecake`). Choosing words will make it easier to remember, but the combinations of letters/numbers will make it harder to guess.

Users must always lock their PC or log off when they leave a PC unattended. This is vital in areas where students can gain easy access to the PC, but is still important in offices that are normally locked as others may well have access to the room and be able to read what is on the screen.

Individuals will be held responsible for all access to/use of the network facilities where they are logged on.

11.1 Multi-Factor Authentication

Account logins for online services such as email, Teams and OneDrive, along with all VPN services are set to request an additional authentication step when using an unknown device (or after 90 days on an authorised device). This authentication can take the form of an approval using an authentication app (recommended), or a code sent by SMS message.

11.2 Network /System Passwords

System wide passwords are the responsibility of the IS&T department and will be changed periodically. System passwords will also be changed if someone who knows it leaves. This may be done as soon as they hand in their notice if deemed necessary.

Passwords will be secure and in line with the advice above.

12 VIRUSES

Staff and Students should be aware of viruses and malware, and the potential damage they can do to PCs, Networks and Servers, and should endeavour to preserve the infrastructures integrity from an attack from such malicious code.

Anti-virus software is provided by WUC for use on all hardware owned by WUC. All media is automatically scanned for viruses, etc. before access to the contents is granted.

Devices bought into WUC should be protected from viruses, etc. through the application of patches, as appropriate, as well as the installation of anti-virus software. It is the owner's responsibility to do this. IS&T can provide assistance/advice if required.

13 STORAGE

13.1 STORAGE LOCATIONS

There are a numberof locations that can use to store files. These, and their intended usage, are outlined below.

13.1.1 PERSONAL USER SPACE - N DRIVE (STAFF & STUDENTS)

Network storage space that is used as the "My Documents" location. Any files saved to the "My Documents" area are stored on the N drive. This allows staff and students to use any PC within WUC and still have access to their own files.

For staff; this should contain only files that are personal to the individual. Storage of departmental work files here should be kept to a minimum as these are best stored on the G drive (see below).

The N drive space is backed up on a daily basis.

13.1.2 SHARED STORAGE SPACE - G DRIVE (STAFF ONLY)

Network storage for department/group/function specific files. Each department can have its own space on this drive and structure the files within it as they see fit. The storage of departmental files in this shared space allows any individual with permissions to continue work in the absence of others without the need to gain access to ther originators N drive.

The structure of a department's area on the G drive is within their control and as such can be defined to individual requirements. It is the department's responsibility to ensure that all files held on the G drive are appropriate and required. Old, out of date and unwanted files should be deleted.

Access to specific areas is controlled by the IS&T department, based upon requests from departmental line managers. Requests to add or remove someone's permissions should be made via either email or an INSERT request (http://insert.writtle.ac.uk) from the owner of the area.

The G drive space is backed up on a daily basis.

13.1.3 TEMPORARY STORAGE - T DRIVE (STAFF & STUDENTS)

The T drive is designed as a temporary area, primarily for transferring files between individuals. Within the staff and student folders there is no access control (students cannot access the T:\staff folder structure). The files can be read, modified and deleted by all. DO NOT use this space for confidential files, or as the only copy of important files.

An overnight routine scans the T drive for files that have not been accessed within the last 14 days and deletes them. It then deletes any empty folders that have been left as a result of the file deletion process.

This area is NOT backed up. Files deleted from here cannot be restored.

13.1.4PC Hard Drive - C Drive (Staff Only)

The local hard dive can be used for storage of files that are not important and can be lost without causing business problems, e.g. audio files. If a hard drive fails, all data kept on this drive may be lost. IS&T will only spend a reasonable amount of time trying to retrieve data from failed PC hard drives.

This area is NOT backed up. Files deleted from here cannot be restored.

13.1.5One Drive

In addition to the users personal N drive and shared G drive, there are also spaces associated with individuals acccounts , knows as their OneDrive, and shared spaces allocated to Teams. Permissions to these areas is under user control and not the responsibility of the IS&T department. Care must be taken when sharing files/folders and assigning permissions that the correct individual is being selected.

13.1.6External Media (USB sticks, external hard drives, CDs)

These are automatically mapped to a drive letter when connected to the PC. Whether personal or WUC owned, care should be taken to avoid connecting to unprotected PCs (i.e. with no anti-virus).

Use of USB stick devices must be kept to a minium as they are potentially unreliable and easy to misplace, leading to potential data loss.

Staff have restricted use of external storage devices, and cannot write to them. Staff who feel the need to access data off campus must consider the use of a VPN connect to access the data direct, or via Writtel File Access (WFA). Confidentiality of student and staff information is paramount and every step must be taken to ensure it remains so. All WUC related data must be removed from the device as soon as it is no longer required.

Disposal of these external devices must be undertaken in line with the IS&T hardware disposal procedures. This will ensure that not only is the equipment recycled in an approved manner, but that the data held on it cannot be accessed. Disposal of CDs, floppy disks must be in a way that will render the media unreadable, e.g. cutting.

These devices are not backed up by WUC.

14 EMAIL

Email services are provided by WUC in support of learning, teaching, research, and the public service mission of the institution and administrative functions that support WUC activities.

Users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner at all times. Email communications should follow the same standards expected in written business communications and public meetings, as in law email messages have the same status as a hard copy letter.

Users are responsible for the actions they take upon receipt of emails. Phishing scam emails can be easily identified by looking for the following signs:

- The language used is often very poor
- They are often unsolicited, e.g. receiving emails at work from HMRC
- Request to open attachments to complete tasks, often .zip files
- Is the email relevant to you or your WUC email address? Emails from banks that you do not bank with asking to confirm details are clearly phishing. Why would your bank email you via any address that is not your home one?
- Emails alleging to come from WUC:
    - Often originate from an address that is **not** a WUC email address, even though it may contain the domain @writtle.ac.uk
    - Contain links you are asked to go to that are to external domains and not any WUC system
    - Often refer to a Help desk, when any email from the IS&T department would make reference to Support Desk

Actions taken by individuals following receipt of such emails (including release of user/password information) may result in disciplinary action.

Special rules apply to emails addressed to all members of staff. Any member of staff wishing to send an email to **All Staff / All Students** must forward their request to Reception who will, if appropriate, forward as appropriate.

In order to reduce the volume of unsolicited and often offensive email ('spam'), all incoming email received from outside WUC is subjected to automated content checking. Incoming messages found to contain viruses are delivered with the virus removed. Messages which are ‘spam’ are not delivered. Any messages which are obviously not ‘spam’ are released for delivery.

WUC may monitor emails to investigate or detect unauthorised use of the email system, or for any other purpose permitted by law. As a result, WUC may collect personal data about the individual sending and/or receiving the email or which is contained in the email. Any personal data collected will be held and processed in accordance with the WUC data management provision under the current Data Protection Act 1998. All queries should initially be referred to the Vice-Chancellor’s Office.

Email communication has the same status as printed material and must therefore be of an acceptable format both in terms of presentation and content. The following points should be considered when constructing an email:

- Is a background necessary? If so, would the inclusion of such a background hinder the reader? **Recommendation: no background**
- Is the font acceptable? **Recommendation: Arial 10/12pt black or any dark colour**
- Is the 'signature' appropriate? **Recommendation: Name, Job Title and contact information only**

15 INTERNET

Access to the Internet from WUC is via the Joint Academic Network (JANET). Use of this service is governed by the JANET Acceptable Use Policy, the latest copy of which can be found on the JANET website https://www.jisc.ac.uk/janet. In particular the following activities are expressly forbidden:

- The creation, transmission or display (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- The creation, transmission or display of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- The creation, transmission or display of defamatory material
- The creation, transmission or display of material such that this infringes the copyright of another person
- The creation, transmission or display of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe

16 AUDITING

All users are reminded of the fact that WUC electronically audits all WUC provided PCs on a regular basis (as deemed necessary by WUC). Sample random or 'spot' audits may be carried out from time-to-time without prior notice.

17 PRINTING & PHOTOCOPYING

17.1 STAFF

Departments will be recharged their printing and photocopying via logging software that records the number of pages printed/copied.

17.2 STUDENTS

Printing and copying will only be allowed when there are sufficient print credits on the account. Credits can be purchased from the Library counter, or online via https://papercut.writtle.ac.uk . Refunds of unused credits will only be given for credit

balances greater than £5 and need to be agreed by the IS&T Manager. It is the responsibility of the student to purchase appropriately.

Credits will only be re-credited back to the student account upon production of a printout that is clearly of poor quality (due to printer failure) or on receipt of an email / telephone request by a member of staff.

Certain situations require the addition of credits to student accounts for the production of work required during a lecture. These requests can be made via the IS&T Support Desk by staff. Care should be taken to only request the required number of credits; and that the students are not being given free printing whilst others have to pay.

18 MOBILE/LAPTOP USERS

All WUC policies apply unequivocally to mobile users. WUC supplied laptops are only supplied with WUC approved software. If auditing software is installed on a WUC laptop, this must not be disabled or removed by the user.

It is recognised that users in the 'field' may require rights to carry out routine administrative functions to the PC and are granted local Administrator Privileges accordingly. These are granted on *trust* proviso, which will be revoked for anybody found abusing the privilege.

Whilst off campus, the equipment must only be used by the WUC employee and those persons who may need to use it in conjunction with the work of the employee, such as:

- academic colleagues (WUC or other institutions)
- technical support staff assisting in agreed installations at other premises

Use by friends and family is not permitted.

19 SUPPORT

19.1 STAFF

All requests for support must be channeled via the IS&T Support Desk without exception, preferably electronically via the Electronic Support Desk (http://insert.writtle.ac.uk). Requests for support will be logged into the IS&T support database and actioned accordingly, stating a level of urgency if applicable. On no account should staff attempt to bypass this policy to expedite their job request, but should instead contact the IS&T Manager.

19.2 STUDENT

All requests for student support for WUC owned equipment must be channeled via the IS&T Support Desk without exception, preferably electronically via the Electronic Support Desk (http://insert.writtle.ac.uk). Requests for support will be logged into the IS&T support database and actioned accordingly, stating a level of urgency if applicable.

WUC can offer support for equipment owned by students. All advice is offered in *good faith* and WUC accepts no liability whatsoever for the consequences for any damage or loss of data thereafter. A form identifying the equipment owner, contact details and an outline of the problem must be completed ensuring that any physical damages are recorded. This form will be used to ensure IS&T know who the owner of the equipment is as well as recording the work undertaken.

20 BACKUP AND RESTORE

20.1 STAFF

All WUC business data should be stored onto a network drive (for example G or N drives), where it will be automatically backed up. Ideally, departmental data should be saved to an appropriate area on the G drive (where it is also available to authorised colleagues), or failing that on your personal space (N drive). Important data must **NOT** be stored solely on your local hard (C) drive (including Desktop), T drive or any other medium which is not backed up. If a local hard drive fails it is very likely that any data stored on it will be unrecoverable.

Staff have a duty of care to ensure that business continuity is preserved, by being aware of the available storage areas and associated backup procedures and ensuring that all vital data is stored securely.

20.2 STUDENT

Students should ensure that important work such as assignments are stored on their N drive.

21 PATCHING

21.1 REMOVAL OF INSECURE SYSTEMS

Whenever any system or device connected to the WUC network presents a perceived risk to University College infrastructure, systems or data, WUC reserves the right to remove that system from the network to avoid potential compromise.

Systems that are removed from the network as a result of insufficient patching will be reconnected only when it can be demonstrated that they have been brought up to date and are no longer a risk.

21.2 SECURE CONFIGURATION AND PATCHING

All devices that connect to the University College network, regardless of operating system, must be protected from attacks which exploit vulnerabilities within the software through the deployment and installation of software and firmware security patches. Security patches must be installed universally across applicable WUC systems, within a reasonable timeframe[1] from their release, in accordance with this policy. Note that in

[1] Two weeks is considered a reasonable timeframe to apply security patches from release date.

exceptional circumstances, it may be required to apply critical security patches immediately to protect against a serious vulnerability.

21.3 Microsoft Windows

- Desktop Patching

  The patching of all WUC devices that connected to the University College network is managed by the IS&T Support Team, providing testing and deployment of all necessary patches to supported versions of Windows[2] within the defined timeframe.

- Deviations to Patch Release

  When an exploit to a vulnerability is published prior to the deployment of a patch, a risk assessment will be carried out by IS&T, to determine whether it is necessary to apply the patch before it has been fully tested. Where the risk of system compromise is considered greater than the impact of deployment of a partially tested patch a decision will be taken to release the patch early.

- Server Patching

  All servers running Microsoft Operating systems should have security patches within two working weeks of the patches being released. If necessary, server restarts will happen outside of core hours.

21.4 Non-Microsoft Platforms

- Patching Information

  All WUC systems that run a non-Microsoft o/s are managed appropriate IS&T teams, and are checked on a regular basis for o/s updates. Publicised vulnerabilities are accessed at the time of publication and when deemed necessary, patching is applied 'out-of-cycle'. Priority of patching critical vulnerabilities must always be given to systems that are available from off campus

- Patching of Core Infrastructure

  IS&T staff will subscribe to appropriate security alert e-mailing lists and monitor trusted sources for notification of any vulnerabilities affecting core infrastructure. Where possible patches will be applied out of core hours, in order to avoid any potential impact on people and services using the infrastructure.

21.5 Bring your own devices (BYOD) and Internet of things (IOT)

All users are responsible for the maintenance of any personal device connected to the network. Where available, devices should be set up receive updates automatically. Where automatic patching is not available, users should ensure that manual checks occur on a regular basis to ensure the device is both up-to-date and still supported.

[2] All WUC Windows devices run supported versions of the O/S

22 BREACHES OF THIS POLICY

IS&T shall be entitled to act upon any breach of this Policy, and shall be entitled to exercise all appropriate remedies, including suspension of the user's network account. Additional sanctions, where deemed necessary, will be conducted through the normal WUC disciplinary procedures.

All breaches of this policy will be reported, in an anonymised form, to the Board of Governors as part of the IS&T Manager annual report.

WUC reserves the right to make variations to the policy as required to be introduced from time to time. However, WUC is not liable under the terms of this policy in the event of failure to adhere to the terms, whether deliberate or otherwise by the users. Individuals should ensure that they familiarise themselves with the contents of the current policy in force.

23 DOCUMENT CONTROL:

Issue	Status	Date	Comments
A	First version	12/08/2004	First issue of complete document.
B	Second version	06/12/2005	Second issue of complete document.
C	Third version	4/3/2008	Third version of complete document.
D	Fourth version	16/12/2014	Fourth version of complete document.
E(1)	Minor change	8/1/2016	Minor change to include references to PREVENT.
E(2)	Minor changes	24/5/2016	Reference to monitoring of usage and password security for ad-hoc systems.
E	Fifth version	10/06/2016	Fifth version following approval at Governors - 10 June 2016.
E	Fifth version	20/7/2016	Revised fifth version incorporating name change to Writtle University College.
F	Sixth version	26/7/2022	Formal ratification of a number of minor changes.