Warrington Collegiate

Warrington Collegiate

IT Security Policy

Policy name:	**IT Security Policy**
Policy reference:	**Pol-ITS-NS**
Created by:	**Director of IT Services**
Approved by:	**Michelle Seeley**
Date of last review:	**July 2016**
Date of next review:	**July 2017**
Revision number:	**1**
Policy links to:	**Data Protection Policy** **Cookie & Privacy Guidelines** **ILT Minimum Expectations Guidelines** **E-learning and ILT Strategy** **Social Media Procedures** **Document Retention Policy**

Warrington Collegiate IT Security Policy
Last Updated: September 2016

Hold down control key and click on section headings to jump to required topic.

Warrington Collegiate IT Security Policy 2
Last Updated: September 2016 2
Purpose 3
Scope 3
Responsibility 3
Computer Usage Policy 4
Rules Governing IT Use 4
JANET Acceptable Use Policy 11
Background 11
Compliance 13
Data Protection Policy 14
Password Policies and Procedures 14
New Computing Accounts 15
Password Security 15
Periodic Expiration 15
Email Policy 19
Access by Warrington Collegiate 19
Confidentiality 20
Prohibited uses 20
Email retention policy 20
Social Networking and Online Safety 21
Safe Data Storage and Disaster Recovery 21
Data Recovery 22
Disaster Recovery 22
Physical and Environmental Security 23
External Security 24
Anti-Virus & Network Security Policy 25
Current Threats 25
Guidelines for users 27
Telephone Systems 28
Purpose 28
Telephone installation and management 28
Right to Privacy and Data Confidentiality 31
Data Protection Act (1998) 31
Human Rights Act (1998) 31
Regulation of Investigatory Powers Act (2000) 31
Disposal of Redundant Equipment 33
Monitoring of this policy 34
Network security 34

Purpose

Warrington Collegiate has a large computer network which in turn forms part of the global Internet. The network and the local computers connected to it may exchange data with any other such device anywhere in the world.

However, such a global network presents some dangers. Among the threats which exist are:

- Breaches of confidentiality, ranging from intrusion of privacy to theft of intellectual property.
- Dissemination of unsolicited, unwanted and possibly offensive and / or illegal material.
- Destruction of information and/or temporary disabling of systems, either accidentally or deliberately.
- Misuse of a publicly funded resource for purposes which do not benefit the organisation and may be illegal in themselves.

From the point of view of Warrington Collegiate, such threats may arise either externally or internally. The Internet, whilst providing huge benefits, constantly increases the threat to Warrington Collegiate and the law makes it clear that the responsibilities for protection are borne by network managers in regulating network traffic. We must take “all reasonable precautions” to protect both our users and our data. Legal responsibility also lies with each user to ensure they do not accidentally or deliberately breach any law or organisation policy.

For all these reasons, a written and enforceable security policy is essential.

Scope

The freedom of network use entails that network managers and their users accept the duty to take all proper precautions to enforce adequate access control, in order to deter and, as far as possible, prevent misuse by others. The failure to act responsibly may have implications for an individual user or even for the whole college.

Responsibility

All aspects of IT Security are the responsibility of Nick Smeltzer, Director of IT Services or a delegated individual(s) within the IT Services team. All queries regarding this policy should be directed to Nick Smeltzer (x4428) in the first instance.

Computer Usage Policy

Warrington Collegiate provides computer facilities and access to its computer networks only for purposes directly connected with the work of the College and with the normal academic activities of staff and students. Individuals have no **right** to use College facilities for any other purpose.

The College reserves the right to exercise control over all activities employing its computer facilities, including examining the content of users' data, such as e-mail, internet access etc., where necessary:

1. For the proper regulation of the College's facilities and performance monitoring and benchmarking;

2. In connection with properly authorised investigations in relation to breaches or alleged breaches of provisions of the College's regulations and the rules on computer use published by IT Services from time to time;

3. To meet legal requirements e.g. the prevention of access to illegal material or for safeguarding of minors or vulnerable adults;

4. To meet our requirements under the Prevent Agenda, preventing access to material that might radicalise people.

Such action will only be undertaken in accordance with guidelines laid down under "Right to Privacy and Data Confidentiality".

Rules Governing IT Use

The following rules govern all use of College IT and network facilities, whether accessed by College property or otherwise:

1. Use is subject at all times to such monitoring as may be necessary for the proper management of the network, or as required to safeguard our staff and students.

2. Persons may only make use of College facilities with proper authorisation. *Proper authorisation* in this context means prior authorisation by IT Services. Any authorisation is subject to compliance with these rules and with the College's regulations will be considered to be terminated by any breach or attempted breach of these rules.

3. Authorisation will be specific to an individual. Any password, authorisation code, etc. given to a user will be for his or her use only. This must be kept secure and not disclosed to or used by any other person.

4. Users are not permitted to use College IT or network facilities for any of the following:

   (a) any unlawful activity;

   (b) the creation, transmission, storage, downloading or display of any offensive, obscene, indecent, or menacing images, data or other material, or any data capable of being resolved into such images or material;

   (c) the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety or to harass another person or system;

   (d) the creation or transmission of defamatory material about any individual or organisation;

   (e) the sending of any email that does not correctly identify the sender of that email or attempts to disguise the identity of the computer from which it was sent;

   (f) the sending of any message appearing to originate from another person or otherwise attempting to impersonate another person;

   (g) the transmission, without proper authorisation, of email to a large number of recipients, unless those recipients have indicated an interest in receiving such email; or the sending or forwarding of email which is intended to encourage the propagation of copies of itself;

   (h) the creation, access or transmission of material in such a way as to infringe a copyright, moral right, trade mark or other intellectual property right;

   (i) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the College without specific authorisation;

   (j) gaining or attempting to gain unauthorised access to any facility or service within or outside the College including to make any attempt to disrupt or impair such a service;

   (k) the deliberate or reckless undertaking of activities such as may result in the following:

      i. the waste of staff effort or network resources, including time on any system accessible via the College's network;

      ii. the corruption or disruption of other users' data;

iii. the violation of the privacy of other users;

iv. the disruption of the work of other users;

v. the introduction or transmission of a virus into the network.

(l) activities not directly connected with employment, study or research in the College (excluding reasonable and limited use for social and recreational purposes where not in breach of these rules or otherwise forbidden) without proper authorisation.

5. Software made available on the College network may only be used subject to the relevant licensing conditions.

6. Users shall treat as confidential any information which may become available to them through the use of such facilities and which is not, on the face of it, intended for unrestricted dissemination; such information shall not be copied, modified, disseminated or used either in whole or in part without the permission of the person or body entitled to give it;

7. No user may use IT facilities to hold or process data relating to a living individual save in accordance with the provisions of current data protection legislation (which in most cases will require the prior consent of the individual or individuals whose data is to be processed). Any person wishing to use IT facilities for such processing is required to inform the College Data Protection Officer in advance and to comply with any guidance given concerning the manner in which the processing may be carried out.

8. Users shall at all times endeavour to comply with guidance issued from time to time by IT Services to assist with the management and efficient use of the network.

9. Connection of computers, whether college, departmental or privately owned, to the College network is subject to the following additional regulations:

(a) Computers connected to the College network by an Ethernet cable must be pre-authorised by IT Services.

(b) The users of computers connected to the College network are responsible for ensuring their security against unauthorised access. The College may temporarily bar access to any computer or network that appears to pose a danger to the security or integrity of any system or network, either within or outside of the College, or which, through a security breach, may bring disrepute to the College.

(c) Users of any service must take all reasonable steps to ensure that that service does not cause an excessive amount of traffic on the College's internal network or its external network links. The College may bar access at any time to computers which appear to cause unreasonable consumption of network resources.

(d) Hosting web pages on computers connected to the College network is not permitted without the knowledge and consent of IT Services. It is not permitted to offer commercial services except with the permission of the IT Services Manager.

(e) Participation in distributed file-sharing (peer to peer) networks is not permitted.

10. In the event that a user is thought to be in breach of one or more of these rules or of College regulations he or she shall be reported to the appropriate officer who may recommend that proceedings be instituted under the College disciplinary procedures. Access to facilities may be withdrawn pending a determination or may be made subject to such conditions as the appropriate officer shall think proper in the circumstances.

Network User Policy

The College has made a major investment in computer and communications technology to promote and support learning and the exchange of information, both within the College and between the College and the rest of the world. These resources are made available in support of the College's mission and institutional goals. Use of these resources should be consistent with this mission and these goals, and this policy.

The relative ease which staff and students of the College can gain access to networked facilities increases the importance of appropriate behaviour by users of computing systems. This policy provides guidelines which, if followed, will ensure that one person's use of facilities does not in any way interfere with the activities of others and does not damage the reputation of the College in the outside world.

As an employee or registered student of the College you have a right to use its computing services at all times, but you must exercise this right in a responsible way. If you misuse computing facilities, you may break College regulations and you may also commit a criminal offence under the Computer Misuse Act.

Authorised Users

1. You have the right to become authorised to use computers and operated by the College but you should not use College computers until you have been authorised to do so.

2. When you join the College as a member of staff or a student you are expected to read and agree to this policy before using any computer system. All users, staff or student, are reminded before every login that they must abide by this policy. Continuing to log in is deemed an acceptance of this policy.

As a safe rule, do not attempt to use any computer unless you have explicit authority to do so. Do not assume that because you can connect to a computer you are allowed to use it.

Software Copyright

1. If you find a copy of any commercial copyrighted or licensed software on the Internet or Network, you cannot legally copy it. These software packages must be purchased or licensed before you can legally use them.

2. Do not attempt to copy software or any information from College or other computer systems for your own personal use unless you have obtained authority to do so from the owner of that software or information.

3. Do not introduce unauthorised copies of software or any other unauthorised information on to College systems.

4. No student or member of staff should copy software off the Internet, even in the case of software deemed to be "Freeware, Shareware or Open Source", unless you have obtained authority to do so.

The College owns site licences for certain software packages; for others, individual licences are purchased. If you are unsure about what you can legally do, please contact IT Services on x4401.

Passwords and Identity

1. It is against College regulations and a criminal offence, if you deliberately use a computer to access any program or information which you are not authorised to access.

2. You must not access or copy information or programs belonging to other users without their permission - preferably in writing.

3. You must not use another user's identity and password, even if they make this information available to you.

4. If a user gives you details of their account, then they are guilty of an offence against the College's regulations.

5. If you are in any doubt whether or not you have permission to access another user's information or programs, you should assume that you do not. You are reminded that attempting to discover another user's password, by any means, is a disciplinary offence within the College and possibly a criminal offence under the Computer Misuse Act.

As a safe rule, do not attempt to use any program or information belonging to another user unless you have explicit authority to do so. Do not assume that because you know another user has a program or information which you wish to access that you are allowed to access it.

Altering another Users' Computer Material

1. It is an offence against College regulations and a criminal offence under the Computer Misuse Act if you alter data, programs, files, electronic mail or any other computer material belonging to another user, without that user's permission. This also applies to the systems data and programs. If you are in any doubt as to whether or not you are allowed to alter another user's computer material do not do so.

2. The wilful introduction of computer viruses or Trojans, which by their nature seek to alter parts of the system, is also an offence under the Computer Misuse Act.

As a safe rule, do not alter computer material belonging to another user unless you have explicit authority to do so. Do not assume that because you are aware of the existence of other users' computer material that you are authorised to alter it.

Payment for Use

1. When you become an authorised user of a College computer, you are only entitled to use it for certain purposes in pursuance of your course or employment in the College.

2. The use of College computing facilities is (in general) free of charge, although some facilities such as the use of printing facilities may require payment.

As a safe rule, do not use a College computer in connection with work for which you receive payment, unless you have explicit authority to do so. Do not assume that because you have been authorised to use a computer for your work within the College you are automatically authorised to use it for paid work.

Administrative data

1. You must not attempt to obtain access to any data relating to the administration of the College, unless you have been explicitly told that you may do so.

2. The College is registered under the Data Protection Act and you have the right, under the Act, to request a copy of the records relating to you, which the College maintains.

As a safe rule, do not attempt to access any data or programs relating to the administration of the College unless you have explicit authority to do so.

Access Preparatory to Other Offences

It is against College regulations and a criminal offence under the Computer Misuse Act if you access computer material as a preparation for some other offence.

JANET Acceptable Use Policy

Background

1. Janet is the name given to an electronic communications network and associated electronic communications networking services and facilities that support the requirements of the UK education and research communities. Organisations in the UK education and research communities use Janet to fulfil and to undertake activities supporting, their missions of providing education, research, and business and community engagement.

2. This Acceptable Use Policy applies in the first instance to any organisation authorised to use Janet (a "**User Organisation**"). It applies also to use of Janet by the User Organisation's own members and all those to whom it otherwise provides with access to Janet (collectively, its "**Members**"). In conjunction with the Janet Security Policy, it is an integral part of the Terms and Conditions for the Provision of the Janet Service (the "**Janet Terms**").

3. The Acceptable Use Policy does not determine the eligibility of any particular organisation or individual to have a connection to and use Janet services. This eligibility is determined by the Janet Eligibility Policy. The Acceptable Use Policy merely defines acceptable and unacceptable use of Janet by those who have been provided with access to Janet services under the terms of the Janet Eligibility Policy.

4. Copies of the Janet Terms, and of the Janet Eligibility and Security Policies may be found on the Janet website.

Acceptable Use

5. A User Organisation and its Members may use Janet for the purpose of communicating with other User Organisations and their Members and with organisations, individuals and services attached to networks which are reachable via Janet. All use of Janet is subject to the Janet Terms.

6. Subject to clauses 8 to 16 below, Janet may be used by a User Organisation and its Members for any lawful activity in furtherance of the missions of the User Organisation. Use by the User Organisation and its Members may be in pursuance of activities for commercial gain as well as for not for profit activities. (See **Note 1**.)

7. It is the responsibility of the User Organisation to ensure that its Members use Janet services in accordance with the Acceptable Use Policy, and with current legislation. (See **Note 2**.)

Unacceptable Use

8. Janet may not be used by a User Organisation or its Members for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities. (See **Note 3**.)

9. Creation / transmission or causing the transmission 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. (See **Note 4**.)

10. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.

11. Creation or transmission of material with the intent to defraud.

12. Creation or transmission of defamatory material.

13. Creation or transmission of material such that this infringes the copyright of another person.

14. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.

15. Deliberate unauthorised access to networked facilities or services. (See **Note 5** and **Note 6**.)

16. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:

    16.1 wasting staff effort or Janet resources, including time on end systems on another User Organisation's network, and the effort of staff involved in the support of those systems;

    16.2 corrupting or destroying other users' data;

    16.3 violating the privacy of other users;

    16.4 disrupting the work of other users;

    16.5 denying service to other users (for example, by overloading of access links or switching equipment, of Janet services, or of services or end systems on another User Organisation's network);

    16.6 continuing to use an item of software or hardware after the Janet Network Operations Centre or its authorised representative has requested that use cease because it is causing disruption to the correct functioning of Janet;

16.7 other misuse of Janet, such as the introduction of “viruses” or other harmful software; or resources on Janet or on another User Organisation’s network.

Access to Other Networks via Janet

17. Where Janet is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network will be regarded as unacceptable use of Janet. Any activity as described in clause 16 above and where applied, either to a user of that network or to an end system attached to it, will also be regarded as unacceptable use of Janet.

18. Any deliberate or persistent breach of industry good practice (as represented by the current standards of the London Internet Exchange) that is likely to damage the reputation of Janet will also be regarded prima facie as unacceptable use of Janet.

Compliance

19. It is the responsibility of the User Organisation to take reasonable steps to ensure its Members’ compliance with the conditions set out in this Policy document and to ensure that unacceptable use of Janet is dealt with promptly and effectively, should it occur. The discharge of this responsibility includes informing all Members of the User Organisation with access to Janet of their obligations in this respect. (See **Note 7**.)

20. Where necessary, service may be withdrawn from the User Organisation, in accordance with the Janet terms. Where violation of these conditions is unlawful, or results in loss or damage to Janet resources or the resources of third parties accessible via Janet, the matter may be referred for legal action.

Explanatory Notes

Note 1: The Acceptable Use Policy does not make any particular statement as to the acceptability of using Janet for activities resulting in commercial gain to the User Organisation, other than this is acceptable, where lawful. However, it should be noted that there are legal constraints applying to a publicly funded User Organisation in such activities. Where the User Organisation is operating as an economic undertaking the issue of State Aid will need to be considered. There is also an issue of the status of both Janet and the User Organisation’s network as private networks. Both are addressed in the Janet Eligibility Policy and more particularly in the Janet factsheets referenced therein.

Note 2: It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of Janet resources on the part of its users and appropriate disciplinary measures taken by their User Organisations.

Note 3: The list of unacceptable activities in this section is not exhaustive. The purpose is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse and potentially unlawful use of a network.

Note 4: It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use and the responsibility for any such approval rests with the User Organisation. Universities UK has provided guidance on handling sensitive research materials.

Note 5: Implicit authorisation may only be presumed where a host and port have been advertised as providing a service (for example by a DNS MX record) and will be considered to have been withdrawn if a complaint from the provider of the service or resource is received either by the User Organisation or by Janet. For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.

Note 6: Where a User Organisation wishes to commission or itself perform a test for vulnerabilities in its IT systems (for example, via "penetration testing") this, as an action authorised by the User Organisation, will not be a breach of clause 15. However, the User Organisation should inform the Janet CSIRT in advance of the test, of the source, nature and timing of the test. This is to avoid wasting the time and resources of the CSIRT in investigating the perceived attack on the User Organisation, or automatically blocking it.

Note 7: In order to discharge this responsibility, it is recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its Members. This should be cast in a form that is compatible with the provisions of this Acceptable Use Policy. Such a statement may refer to or include material from this document. If material is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of the Janet Acceptable Use Policy. The Janet Service Desk can advise on this aspect if required.

Data Protection Policy

Please refer to the Warrington Collegiate Data Protection Policy which can be found on the Warrington Collegiate website.

Password Policies and Procedures

This section summarises Warrington Colligates password policies and procedures. The intent of these policies is to provide a safe computing environment on the college's computers and prevent security compromises on these systems.

New Computing Accounts

Student accounts

Student accounts are automatically generated for all new students upon registration. These accounts consist of a username and password and provide access to shared resources and a private home directory. The password will be set by IT Services but a student may change it to a password of their own choosing. The password will consist of at least 8 characters and can be changed by the user at any time.

Staff accounts

Staff accounts are generated as a new member of staff starts at the college. These accounts consist of a username and password and provide access to shared resources, a private home directory, email and other network resources deemed necessary for the particular job function. The password will be set by IT Services but pre-expired so that the member of staff is prompted to change it to a password of their own choosing. The password will consist of at least 8 alpha-numeric characters and will need changing occasionally (see note on password security). Before the username and password are issued, the member of staff is required to sign an application form, agree to this policy and have it countersigned by their line manager.

Password Security

One of the easiest ways for a person to hack a computer system is by gaining access via a user's personal account. This is frequently possible when accounts have easily guessed passwords (e.g. when the password is the same as the username or the person's first or last name, etc.) At best, an insecure password may compromise a single user's data, and at worst it may compromise the entire system. You should be aware that you are solely responsible for your account, and may have it revoked if it is misused. Therefore, it is in your best interest to keep your account as secure as possible. The password is your first line of defence, so don't reveal your password to anyone else.

Periodic Expiration

Some organisations opt to change their passwords every 30 days or every 90 days (i.e. once per term). This often results in password re-use by adding an extra number and then incrementing it by one each change or worse still, writing the password down on a post-it note next to the computer monitor. Warrington Collegiate are of the opinion that infrequent changes of a more secure password is the best policy. Therefore, staff should have an alpha-numeric password that they are forced to change infrequently. All student passwords last the duration of the academic year whereupon the accounts

are deleted and new accounts created. When your password expires, you will be forced to change your password at the next login. You will have 3 grace logins to change your password, being prompted each time until you do. Failure to change your password will result in your account automatically being locked.

In cases where IT Services have a legitimate need to change a user's password, the password will be set to expire immediately, prompting for a password change when the user next logs in. IT Services do not hold **any** passwords for any users except those accounts used within IT Services.

Selecting a "Good" Password

Password cracking tools exist that can make light work of breaking simple passwords that are based on dictionary words. A copy of the English dictionary is loaded in to them and they can try every word in the dictionary within a few seconds to a few minutes. The can then go through the same words, swapping some letters for numbers.

Therefore, when selecting a new password, please follow these guidelines:

- The password must be at least 8 characters long.
- Passwords should contain a mix of numbers and letters.
- You should not choose any word that is in a dictionary, or any names, places, or personal information like your birth date.
- Converting an easy-to-remember phrase into an acronym with symbols is also a good strategy: "I like to keep my password nice and secure" could be abbreviated to 'iltkmpnas', and then by changing a letter to a number, would become a password of **i1tkmpnas** which is a good, non-guessable password.

Mathematically, as the length of the password increases, the number of possible character combinations (and therefore the password strength) increases exponentially, as shown in the table below. Password strength is increased due to the longer time required to generate all possible combinations for a given number of characters.

Number of Characters in Password	Possible Combinations (Letters A-Z Only)	Possible Combinations (Letters A-Z, with numbers 0-9)
1	26	36
2	676	1,296
3	17,576	46,656
4	456,976	1,679,616
5	11,881,376	60,466,176
6	308,915,776	2,176,782,336
7	8,031,810,176	78,364,164,096
8	208,827,064,576	2,821,109,907,456
9	5,429,503,678,976	101,559,956,668,416
10	141,167,095,653,376	3,656,158,440,062,980

Changing Your Password Manually

1. Log into your account.
2. Press Ctrl-Alt-Del
3. Select Change a Password
4. Follow the on-screen instructions to complete your request.

Requesting a Password Change in Person

If you have forgotten your password or are unable to use the previously mentioned methods, you should come in to the IT Services Office, A133 and request a password change in person. You must bring a Photo ID in order to make a password change request.

Access Control

All user security is managed by IT Services within an Active Directory environment. This allows for the creation of a flexible and very secure network operating system. No facilities exist outside of IT Services for users to manage or create their own accounts.

The network design is documented and stored securely.

Users will only be allowed access to information required as part of their employment and study. User rights will be strictly controlled and administered

by the IT Services section. Access to shared Network drives will be administered by the IT Services section and closely monitored. Staff applying for access to shared drives must make an application in writing to the IT Services section.

Security utilities will be executed regularly on all Networked systems to identify any excessive rights granted to users of the system. Should the security utilities identify any accounts that have not been used for 6 months then a check on employment status with the Human Resources section will be made.

Email Policy

The email system is provided to staff/students at Warrington Colligates expense to assist staff/students in carrying out Warrington Collegiate business. Warrington Collegiate treats all information transmitted through or stored in its computer system, including e-mail messages as Warrington Collegiate business information. All email messages and documents created on the System are and remain the property of Warrington Collegiate.

The following items should be noted when communicating by email:

1. E-mail messages should be clear, courteous, professional and business-like;

2. Please remember that the Internet is not a 100% secure communications medium. Although we have taken steps to ensure that the email system and attachments are free from any virus, we advise that in keeping with good computing practice the recipient should never open any attachment unless they are actually expecting it.

3. Delete unwanted or junk mail immediately.

4. Do not open attachments from unsolicited mail or click on any links.

5. Emails can get lost, the system is not able to interpret spelling mistakes, dots in the wrong places, etc. If the email address is not exactly correct, it will either be undeliverable or delivered to the wrong person. Equally, incoming emails will get lost if you are not correctly identified in the address.

6. Do not assume that your email has been received if the matter is urgent, receipts may work internally, but might not be recognised at the receiving end. If in doubt, phone through to check that it has been opened by the intended recipient. Email is not always fast, it will depend on the software used on both sides, the service providers and the load on the network.

7. Certain information about Warrington Collegiate must never be sent by email. This includes the following: personal staff details, payroll information, accounts information and other private and confidential information. If in doubt, ask IT Services.

Access by Warrington Collegiate

Warrington Collegiate has the right to access, review, copy, modify and delete any information in the computer system, including email. Warrington Collegiate also has the right to access, review, copy, modify or delete all such information as it deems appropriate. Information and email created by staff/students using the computer for personal purposes will be treated the

same as other information and email; ie Warrington Collegiate has the right to access, review, copy, modify, delete or disclose such information.

Confidentiality

Email messages shall be treated as confidential by other staff/students and accessed only by the intended recipient. Staff/students are not authorised to retrieve and read any email messages that are not addressed to them.

Everyone must exercise caution in transmitting confidential company information because of the reduced effort required in electronic communication. Confidential information should never be transmitted or forwarded to external individuals or companies that are not authorised to receive the information. Confidential information should not be sent to other staff/students inside the company who do not need to know the information.

Always use care in addressing email messages to make sure that the messages are not inadvertently sent to the wrong person or sent outside the company. Exercise care when using distribution lists and take measures to ensure that the lists are current. The confidentiality of any message should not be assumed. Even when a message is deleted, it is still possible to retrieve and use that message either internally or by a third party.

Prohibited uses

The email system is not to be used to create or disseminate any offensive or disruptive messages. Among those that are considered offensive are any messages which contain sexual implications, racial slurs, gender specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability. The email system should not be used to promote chain letters, or other similar types of activities.

The email system may not be used to solicit or proselytise for commercial ventures, religious or political causes, outside organisations, or other non-job related solicitations.

Email retention policy

Warrington Collegiate strongly discourages the storage of large numbers of email messages for the following reasons:

1. Email messages frequently contain confidential information;

2. retention of messages fills up large amounts of storage space on the network and personal computers which slows performance;

3. to expedite searches of the network, backups, or individual personal computers for genuinely important documents.

Staff/students shall:

Promptly delete any e-mail messages they send or receive that no longer require and or are not necessary to an ongoing activity;

Audit their stored messages regularly to identify messages that are no longer needed and delete them.

Warrington Collegiate shall automatically delete all emails more than 2 weeks old from users Trash folders and shall impose maximum storage capacities on user's mailboxes (currently 3GB per user).

Social Networking and Online Safety

Please refer to the Social Media Procedures which can be found on the Warrington Collegiate website.

Safe Data Storage and Disaster Recovery

Hard Disks

Whenever you work on a computer you are going to produce documents in one form or another, from word processing to databases until they are saved on to some form of media they are considered volatile and would be lost if the computer was turned off or crashed. All work should be saved to the network as that is the most reliable way of storing your data. Storing your data on your pc is a risk. PCs have a 10% failure rate over their lifetime and if yours fails and your data is on it, your data has gone.

USB Disks/Pens

USB disks are a flexible way of storing and carrying data but they bring with them their own problems. If you rely on a USB disk for day to day storage of your data and then lose the USB disk, you lose all your work. But you also run the risk of this data falling in to someone else's hands. If you have confidential data relating to other individuals, you could face fines of up to £50,000 under the Data Protection Act. Therefore, our advice is to NOT use USB disks at all, but to use Cloud Storage for transferring files. If you do use USB disks, just use them for temporary storage of files you are transferring and not for permanent storage. You should consider encrypting all data on USB drives in case you lose it and you MUST use encryption is you store sensitive data.

Cloud Storage

Each member or staff and each student is entitled to 1TB of cloud storage which is available to you wherever you are in the world, provided you have an internet connection. Cloud storage is much more secure and reliable than USB storage, indeed the only reason for not using cloud storage completely is that its speed is a lot slower than local networked storage. Cloud storage

should be used for transferring files between home and college and for a backup of all your personal and work files.

Network Storage

Each server has multiple disks available to it with redundant disks online and ready to take over from any failure. If we lose a disk, an online spare will kick in. We also have multiple online servers which in practice means that we can lose either an entire server (or more) or an entire disk (or more) without any loss of data or any downtime for our users. Providing we do not lose our server room, our data is highly protected and resilient.

To insure against loss of our server room, all data stores are backed up daily or weekly (depending on the criticality of the system) to disks in a physically separate building. We back up one set of servers each day until all the servers are backed up by the end of the week. We cannot backup the data every day due to the sheer amount of data we have and the length of time the backups take. In addition, core servers are periodically archived so that we can restore data from further back in the past in the event of a disaster.

Data Recovery

If a file or files need to be recovered, it can be done in a number of ways:

- Recovered from the network drive the file resided in (previous versions)
- Recovered from backup

IT Services regularly test the system at least weekly by deleting random files (of our creation) and then recovering them.

Disaster Recovery

The primary source of data failure is caused by power outages or power spikes. All core network equipment is on a “clean” supply dedicated just to the computer equipment. UPS’s provide another line of defence, providing backup battery power for at least 45 minutes in the event of a total power failure. As the battery exhausts, the systems close down in an orderly fashion.

IT Services periodically (once per year) carry out a disaster recovery exercise and turn off, for example, the MIS server and restore its data on to a test server. We then ask the staff to test the system to see if they can notice any difference. Each of the key systems are tested in this way (listed in order of criticality):

- MIS servers
- Finance servers
- Staff servers
- Student servers
- Mail servers
- Internet servers

Physical and Environmental Security

The very nature of an open access college presents problems with the physical security of computers, however all of the core systems are behind locked doors.

The fileservers and router equipment are located behind two locked doors. Cleaning staff and security staff do not hold a key, any emergency access out of hours is obtained through the usual IT Emergency Contact procedures. In addition, there is a key code access lock on the server door.

Backups are stored in a physically separate building that only IT Services staff have access to.

The IT Services safe is a combination safe and archived data. The safe is located in a locked office in a separate building to the server room.

Asset classification and control

The Finance and IT sections are responsible for maintaining the accuracy of an organisational asset register. IT Services maintain a separate and more detailed record of all computer related hardware and software including, but not limited to, serial numbers and machine specifications. Information will be amended prior to disposal or relocation computer equipment. Assets will be defined using the Institute labelling procedure and in accordance will financial regulations and policy.

Resilience

All core routers, switches and servers contain an element of resilience built in. All programming of routers and servers is documented and stored securely enabling a failed item to be returned to service with minimum down time.

Personnel

The Human Resources team will be responsible for documenting job definitions and performing verification checks on permanent staff at the time of job applications. IT Services staff will be required to sign a confidentiality agreement as part of their conditions of employment. The confidentiality agreement will contain details of the employee's responsibility for information security.

Security Incidents

The IT Services section will be responsible for continual risk assessment of all computer systems. Security issues will be documented and appropriate action taken. Violation of security policy by both staff and students will be dealt with through formal disciplinary procedure.

Movement of Equipment or Data

Staff/students will be made aware of their responsibilities regarding sensitive information left on unattended screens. Equipment, information or software belonging to the Institute will not be removed without full knowledge of the IT Services section. A record will be held by the IT services section of IT equipment loaned to staff and students.

Documentation and Change

Any changes to computing facilities and systems will be documented and monitored. Development and testing facilities will be located in a separate environment to the operational environment. New equipment brought on-line is fully tested on a physically separate network testing room within IT Services.

Housekeeping

Daily housekeeping is carried out on all servers and systems minimising downtime for users. Where downtime is unavoidable, as much notice as possible is given and users' needs accommodated. IT Services aim to provide 99% uptime on all systems.

External Security

The College operates a firewall. The firewall logs are checked at least daily and action taken where necessary. In addition, IT Services staff will periodically test the firewalls external security running security utilities from outside internet connections. Likewise, the internal security is tested in a similar manner. The firewall will alert us by immediate email if it considers a threat is imminent.

Anti-Virus & Network Security Policy

[Note: This section is regularly updated outside of the policy review schedule to take in to account latest threats and trends]

Current Threats

Since 2015 (and as at September 2016) the current threats include:

- Ransomware and evolving malware generally
- VIP Spoof ware
- SMB's becoming a target for cybercriminals
- Android and IOS threats
- DDOS attacks and the Internet of Things

Ransomware

Ransomware has become so prolific and high profile that it is now a household term. It has become increasing common because of email attachments tricking the end user into opening the malicious file. Typically, they are either a hyperlink to a website or have an attached word.doc file. They can pretend to be tax rebates, postal tracking links or password reset links supposedly from your IT team. Once opened or clicked on, they scramble all your files and are so successful that they have proved impossible to recover from. With so many new variants released every day, we find several get through our defences and are later picked up by the anti-virus systems after an update. Only because of good user education and the fact that we block the most commonly used transmission methods have we escaped a serious infection.

VIP Spoof ware

VIP Spoof ware is where an attacker or hacker spoofs emails allegedly from key individuals within a user's own company. A typical example is an email to the finance team from the Finance Director or Chief Executive asking for a transfer of funds. There have been several attempts at this, but good user education can usually spot it and if in doubt, it's quite simple (in a small organisation like ours) to speak to the person concerned over the phone. Information on a company can come from public sources like Director lists and annual reports, but often comes from social engineering.

SMB's as a target

Once, only large household names were open to attack Microsoft, Sony, Yahoo etc. However, the threat landscape has changed and in the UK, some 75% of SMB's have been the subject of a cyber-attack of some sort. Again, this can be a physical attack – breaking in to our network via a security vulnerability or it could be social engineering i.e. phoning up a user pretending to be from the helpdesk and asking for a password change.

Just like your bank, we will never ask you for your password and if you are in any doubt about divulging any sort of information, just phone the Helpdesk on x4401 or email itservices@warrington.ac.uk and one of us will advise.

Android and IOS threats

Whilst there has always been a threat to Android phones, this usually meant the user deliberately circumventing the devices security and installing non-trusted apps. Now, however, app writes are going to extreme lengths to hide their payload so that they make it on to the legitimate Google Play store.

The same applies to IOS. IOS viruses used to be unheard of, but are becoming more prolific as the writers find ways of hiding their payload from Apple.

DDOS attacks and the Internet of Things

One of the most common forms of attack that affects us on probably a monthly basis is a Distributed Denial of Service attack. As the name suggests, a denial of service attack is just that, it is an attack that forces some or all of an organisations internet facing business off line. A distributed one is simply an attack that is co-ordinated from many separate sources.

When we suffer a DDOS attack, we tend to find our web surfing (i.e. internet bandwidth) slows right down and sometimes stops working altogether. Attackers sometimes do this for payment (i.e. targeting a competitor's company or targeting a country's infrastructure), but normally it is just vandalism "for fun" or to show off that they can take someone down. The normal targets for attacks that affect us are various points on the Janet Network and the victims are normally anywhere between 10-100 colleges, Universities and local authorities. When an attack is spotted, it is normally mitigated within an hour or so and they normally never last longer than half a day.

One of the largest attacks of 2016 involved compromised Internet of Things (IOT) devices – e.g. fridges, TV's, cameras and any other internet connected device with poor security. Until manufacturers get better at in-built security and users change default passwords, this is going to be more common in 2017.

Hoax Viruses

Whilst viruses pose a real threat to users of computer systems, many users don't realise that virus hoaxes are more of a problem. Anti-virus software protects systems against all known viruses and provide up-dates for new ones, hoaxes cannot be protected against and consume huge amounts of network bandwidth and disk space when all users send a copy of the hoax to "everyone in their address book".

"You shall not forward any virus warnings of any kind to anyone other than IT Services. It doesn't matter if the virus warnings have come from an anti-virus vendor or been confirmed by any large computer company or your best friend. All virus warnings should be sent to IT Services, and IT Services alone. It is IT Service's job to send round all virus warnings, and a virus warning that comes from any other source should be ignored."

Guidelines for users

Of course new viruses can sneak through before the anti-virus companies have had chance to write an update, so the following guide will prevent infections:

1. Get in to the habit of sharing files using DOCX as a file format for Word Documents (XLSX for Excel and PPTX for PowerPoint), do not use the older DOC or RTF formats as these can harbour viruses. Warrington collegiate have blocked all RTF and DOC files from being received from external organisations. Whilst this might mean some impact on a user's day to day business, we feel the benefits outweigh the disadvantages.

2. Do NOT click on any link in an email or open any attachment to an email unless you are specifically expecting.

3. Any email you weren't expecting should be treated with suspicion, even if it comes from someone you know as sender addresses are easily faked.

4. Do not download anything from the internet. Legitimate programs are often booby-trapped to contain viruses, spyware or ransomware.

5. If in doubt, always ask your IT department for advice, do not open the file or email.

6. If you think you have been infected with a virus inform your IT department immediately. Do not panic or interrupt other users.

7. Any virus warnings or hoaxes should be sent to the IT department who can confirm whether or not it is genuine. Do not forward these warnings to anyone else; unless you are signed up to an official virus alert service it is unlikely to be a genuine warning.

8. If you have to work at home, ensure that you follow the same procedures there as you do at work. Viruses can easily be brought into an organisation along with work that has been done on a home PC.

9. Anti-virus software will prevent the vast majority of viruses from entering an organisation but it is not fool-proof. It is your responsibility to ensure that you don't get infected with a computer virus.

Telephone Systems

Purpose

This section outlines Warrington Colligates policy on telephones and communications. It covers telephone installation, usage and monitoring and covers the purchase and use of mobile phones. All users should be aware of this policy, their responsibilities and any legal obligations.

Warrington Collegiate is committed to the appropriate use of Information and Communications Technology, which includes the telephone system. The college requires users to accept all IT policies and associated procedures. These policies can be found under the IT Services section of the college Intranet.

Telephone installation and management

IT Services will be responsible for the installation of telephone cables, phones and all associated equipment. Under no circumstances should a third party, without authorisation from IT Services, be allowed to install or access any telephone equipment on college premises.

IT Services will be responsible for the purchase of all contract mobile phones. However, monthly payment for such phones will be made by the user or department, not IT Services. “Pay as you Go” phones are exempt from this policy.

IT Services will provide a voice mail mailbox for each extension unless there is a valid reason not to.

The access rights of each telephone handset will be classified as follows:

- Receive calls only – no dial out.
- College internal access – phone college extensions only.
- National access – phone anywhere in the UK.
- International access – phone anywhere in the world.

Normally, only a head of department or senior manager has the ability to make international calls. Users that need to make an international call should dial 0 for reception and ask reception to make the call for them. This is logged against the user making the request.

Phones in public areas (corridors etc.) are classified as college internal access only and are not able to make external calls.

Mobile telephones

Contract mobile phones should be avoided at all costs due to the financial overhead that they place on the college. Where a contract mobile phone is the only option, the department the user is in is responsible for paying all charges associated with its use.

“Pay As You Go” phones may be purchased outright by any user in any department. IT Services will offer advice on the best solution for a given purpose. Again, the user or department is required to pay for any vouchers or other costs.

IT Services should be advised of the telephone number of all mobile phones, contract or Pay As You Go. This is to enable us to enter their details on to our call logging system (see section on Monitoring below) so that they show up as calls to college phones rather than unknown mobiles.

Users should avoid calling mobile phones unless there is a critical business need to do so. Calls between college extensions are free, but calls to mobile phones (including those owned by the college) cost a significant amount of money each year. IT Services accept that there is a business need for calling mobile phones, but reserves the right to recharge the department if costs become excessive.

Some users, particularly in support areas, have the facility to have their office phone divert to their mobile whilst they are away from the office. The college accepts the business need for doing this, but requests that users that have this feature only use it when necessary and remember to un-divert their phone when back in the office to prevent the college from needlessly being charged for a call to a mobile when a call to an internal extension is free.

Users should remember that mobile phones, contract or Pay As You Go, remain the property of the college and should be returned to the college as a user leaves.

Any mobile phone that is lost or stolen must be reported to IT Services immediately so that it’s use can be blocked and tracking activated where possible.

Use of mobile phones whilst driving should be avoided at all costs. It is a specific offence to use a mobile phone whilst driving unless a hands free kit is used, but the college’s advice is not to use your phone whilst driving.

Personal usage

To comply with the Human Rights Act, staff have a right to “limited personal use” of the phone system but the college also has a right to charge the user for any personal calls. However, the college will not charge users for **occasional** personal calls where the call destination is to a **landline** and the call duration is **5 minutes or less**. All personal calls to **mobile** phones **will** be

charged for and all personal calls of more than **5 minutes** in duration **will** be charged for. Users can seek advice from IT Services to find out the cost of a call and can then make payment directly to Finance.

IT Services monitor the phone records (see section on monitoring below), but are not able to differentiate between personal and business calls. Therefore, we may approach a user or a department head to seek clarification on a particular number to ascertain if calls made to it were of a business or personal nature.

Monitoring and logging of calls

The college has a legitimate right and business need to log details of all calls made from college telephony equipment to other college extensions or outside numbers. The college also logs all incoming calls to all college numbers. This logging includes:

Number called from, number called to, call duration, call cost.

Logging is carried out for the following reasons:

- To act as a comparison checker against our itemised telephone bill to make sure we are not being incorrectly charged by our telecommunications provider.

- To prevent, detect and minimise unacceptable behaviour on the phone system.

- To prevent, detect and minimise system problems.

Call detail information obtained by logging will not be made publicly available, but will be available on request as follows:

- All call information available to senior management on request.

- All call information available to the police should the need arise and taking account of the Data Protection Act.

- All call information for a department available to the department head on request.

- All call information for a particular extension available to the user of that extension.

Right to Privacy and Data Confidentiality

Data Protection Act (1998)

The Data Protection Act (1998) requires the college to keep personal data safe and secure and to prevent access to it to unauthorised individuals, whilst allowing access to those that require it.

Human Rights Act (1998)

The Human Rights Act (1998) gives staff/students the right to expect a certain amount of privacy at work, including, but not limited to, electronic storage of data and use of telephone and email systems.

Regulation of Investigatory Powers Act (2000)

The Regulation of Investigatory Powers Act (2000) however, undermines some elements of both the Data Protection Act and the Human Rights Act by allowing an employer to monitor telephone calls, email messages and files where the employer has a legitimate need to do so.

Therefore, staff/students of Warrington Collegiate cannot expect a right of privacy in either their network areas, email messages or telephone conversations. It should be made clear however, that only named individuals (currently: N Smeltzer and G Robinson) within IT Services will have the rights to monitor information and then only in the following circumstances:

1. When asked to monitor an employee (and given a legitimate reason) by the Leadership Team

2. When asked to monitor a student (and given a legitimate reason) by any member of academic staff.

3. To monitor network performance, security and data storage quotas.

Examples of what is allowed under the RIP Act (2000)

1. A member of the Leadership Team has reason to believe a member of staff is conducting paid personal business from Warrington Collegiate machines. IT Services are requested to check the staff email and personal files.

2. IT Services conduct monitoring of the email/network system to produce traffic statistics to aid in troubleshooting problems or to make further enhancements.

3. IT Services conduct file searches looking for copy protected media.

Examples of what is not allowed under the RIP Act (2000)

1. A member of staff wants access to another staff's files whilst they are on holiday. The Data Protection Act (1998) and the Human Rights Act (1998) both prevent this without the consent on the individual concerned or a legitimate business case made by a senior manager.

2. IT Services staff open and read personnel files held by Human Resources Staff. Again, both the Data Protection Act (1998) and the Human Rights Act (1998) both prevent this without the consent of the individual.

Any monitoring undertaken will be for as short a duration as possible, then only carried out in pairs for security and under no circumstances will any information not directly relating to the reason for the investigation, be disclosed to any party.

Disposal of Redundant Equipment

Any machines that reach the end of their useful life and are owned rather than leased are disposed of following the guidelines in this policy.

Only IT Services staff may decide which machines are for disposal and only IT Services staff may actually dispose of machines.

During 2003, it will become an offence under new EC regulations to dispose of PC's and associated equipment through normal waste disposal means. It is also an offence under the Data Protection Act (1998) to allow confidential data outside of the College. Therefore, IT Services should follow the guidelines below when disposing of machines:

1. Machines for disposal must either be:
    a. 4 years old (or more) and owned, not leased.
    b. Broken beyond economical repair if less than 4 years old.

2. Asset numbers must be taken and recorded with both the IT Helpdesk and Finance to make sure both record the fact that the machines have been disposed of.

3. All machines must be recycled internally where possible. That includes, but is not limited to, re-using parts and re-using whole machines elsewhere in the college or for testing purposes.

4. Machines that have no useful purpose within the college are to have their hard disks securely erased and then disposed of via EBay if there is any re-saleable value in them or via a CPC-approved computer recyclers.

Monitoring of this policy

Compliance with and adherence to this policy are essential for the correct functioning of Warrington Collegiate so information and communication technology usage is monitored in the following ways:

Network security

All successful logins to the network are monitored. Details include: date, time, machine used, username, network address. All unsuccessful login attempts are logged with the same level of detail, but this time an alert is sent to IT Services staff. The firewall is configured to log all critical incidents. Critical incidents include Denial of Service attacks, multiple guessing of passwords, brute force attacks, port scanning. The firewall logs are reviewed on a daily basis. Network areas are periodically checked by an automated checker for the presence of any hacking-type utilities. Further, all account creation requests are logged and stored together with a copy of the authorising signature.

Server and router uptime

All servers, routers (internet access etc.) and other key systems are monitored once every minute. In the event of an item failing to reply, 3 more requests are sent in quick succession. If it still fails to reply, it is presumed to be down and an emergency alert is broadcast to IT Services staff by pop-up message and email message.

Internet access

All websites visited are logged. Details include: username, URL, source IP address (on our network), destination IP address (on the internet) date and time. The logs are periodically checked for occurrences of certain key words. Any found leads to further investigation.

Telephone systems

All calls in to and out of the college are logged (not monitored). Details include: source telephone number, destination telephone number, date, time, duration of call, class of service (i.e. mobile, national rate, local call etc.), cost of call.

Anti-virus system

All virus attacks are logged. Details include: name of virus, user's machine or users email address, source of virus. Unlike most of the other information collated, this information is shared with Sophos to help fight the spread of viruses.

For further information on any part of this policy, please contact the Director of IT Services on x4428.