Policy & Procedure	Policy On Acceptable Use Of IT
Policy Area	IT
Version Number	01
Approving Committee	SMT
Date of Approval	13 December 2016
Date of Equality Impact Assessment	17 September 2015
Date of Review	01 December 2019
Responsible Senior Manager	David Black (Director of IT)

History of Amendments

Date	Version/Pages/Sections Affected	Summary of changes

Policy Statement

All College policies are in a standard format and a consistent approach is taken in the production, monitoring and review process. The current official version of every policy is the one that is published on the staff intranet under the section headed Policies and Procedures. A policy becomes effective as soon as it is published on the staff intranet. If a policy is to be published in other locations then where possible it should be hyperlinked to the definitive version on the staff intranet.

Procedures associated with observing the policy are contained within this policy document. Template documents associated with this policy are located in the Forms section of the Staff Intranet.

Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

Contents

Policy on Acceptable Use of IT

1. Policy Statement

It is an aim of the College to encourage the responsible use of Information Technology [IT] by and for all of its stakeholders. This policy aims to reduce the likelihood of legal liability for the College or its IT users, as well as reducing the likelihood of any breach in security practices or regulations that could jeopardise the business and commercial reputation of the College.

The College recognises the significant benefits in making Information Technologies available to staff, students and other stakeholders and seeks to minimise barriers to access whilst ensuring that systems and users are adequately protected. The College is also aware that there are potential issues associated with IT use and that all users will therefore benefit from having the Colleges' guiding rules and principles set out in advance of use.

This policy, while providing guidance regarding what is and what is not acceptable use of the IT hardware and systems provided for stakeholders, cannot lay down rules to cover every possible situation. Instead the policy aims to set out the College's approach and detail the general principles that apply when using the Information Technology systems and hardware provided by the College.

These guidelines give a clear indication to users whether or not their intended use of the system would be appropriate and acceptable.

2. Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

3. Purpose

This policy details the College's rules and guidelines for the acceptable use of Information Technology systems and hardware.

West College Scotland will provide access to appropriate elements of its IT hardware and systems, to stakeholders by arrangement. This access will be as part of the College operational activities or to support or manage the College's operational activities.
West College Scotland reserves the right to withdraw this access at any time and without prior notice, subject to the terms of the policy.

4. Scope

This policy applies to all students, employees, Board members, contractors, supplier support personnel, visitors or others given authorised access to the systems and infrastructure provided by West College Scotland.
This policy covers all computer hardware, software, data communication systems and all other components connected to or associated with these systems, which include, but is not limited to, personal and laptop computers, printers, servers and storage arrays, software applications, databases, e-mail systems and intranet or Internet based resource or service.

5. Policy Acceptance

The mode of acceptance will vary by category of user. The policy is accepted by staff on taking up employment, and by students during the enrolment processes or at first attendance.
All users are reminded of and accept their obligation to adhere to College IT policies when they are presented with, and accept, the '*Access Permitted to Authorised Users Only'* information message during the initial part of the computer logon process.
The policy will be available on the College website for reference by any prospective student or employee.

6. Access To Systems

The College provides automatic access to its IT systems and resources to all current employees, including Board members, and enrolled students.

Employees and Board members are provided with access on taking up post. Access is for individual use and appropriate to role.

During periods away from College i.e. long term sick, maternity or sabbatical; the user account permissions will be adapted to permit access to on-line communication and employee information resources.

Access may be suspended if an individual comes under disciplinary investigation or suspension and access will be removed completely when an appointment terminates.

Students are provided with access from the point of enrolment. Access is for individual use and customised around a course of study. It may be suspended during periods of forced absence (e.g. criminal proceedings) and is removed completely on course completion.

The College may also make available access to visitors or contractors in specific circumstances and for specific purposes.

7. Conduct And Acceptable Use

The College provides IT access and resource to support its teaching and learning aims. Users are encouraged to use IT resources productively but in doing so are expected to;

1. Behave responsibly and ethically when using IT resource.
2. Respect the privacy and access rights of others.
3. Maintain and protect the security and secrecy of their systems access credentials.
4. Maintain the integrity of College data.
5. Give due thought to security and privacy when handling College or personal data.
6. Seek guidance from within the IT department, if in doubt over an intended action.

8. Acceptable Personal Use

The College's IT resources are made available to stakeholders to deliver and support the teaching and learning process. The College recognises that personal use is possible and accepts this, so long as the personal use;

1. Is reasonable in duration
2. Does not interfere with, or detract from, teaching, learning, employment or course commitments of the individual or others.

3. Complies with all IT policies in force, including this one
4. Does not incur an unreasonable direct cost on consumable expenditure or resources (*i.e. when printing personal material using College equipment*)

9. Internet Connectivity

The College connects to the Internet as part of the wider Joint Academic Network [JANET] community. When making use of Internet based resources, users are additionally bound by the terms of the Janet Acceptable Use policy.
Full details can be found here - https://community.ja.net/library/acceptable-use-policy

10. Misuse

To provide guidance to users, the College deems the following behaviours to be unacceptable use of the College's IT resources;

1. Creation or transmission of images, data or other material; or any data hidden or encrypted that is obscene or indecent.
2. Creation or transmission of offensive material relating to a protected charectistic as defined under the Equality Act 2010.
3. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
4. Creation or transmission of material with the intent to defraud.
5. Creation or transmission of material found to be defamatory.
6. Creation or transmission of material such that this infringes the copyright of another person.
7. Creation or transmission of unsolicited bulk or unsolicited marketing material, or a combination of both.
8. Creation or transmission of chain, junk or other unsolicited private messages using email or any other means.
9. Installing unauthorised or unlicensed software.
10. Vandalising, damaging, disconnecting or otherwise removing College IT equipment.
11. Attaching unauthorised equipment to the College network.

12. Deliberate unauthorised access to networked facilities or services. This includes attempts to circumvent security systems or filters, and unauthorised attempts to access data, either College administered data or the personal data belonging to an individual.
13. Any action which is likely, intended or otherwise, to damage the reputation of West College Scotland.
14. Deliberate activities having any of the following characteristics:
    a. Wasting staff effort or network resources;
    b. Corrupting or destroying other users' data;
    c. Violating the privacy of other users;
    d. Publishing personal information relating to another individual or group;
    e. Disrupting the work of other users;
    f. Harassing or bullying of other users;
    g. Denying service access to other users;
    h. Continued use of software or hardware on the College's IT systems after an instruction to cease has been issued to a user;
    i. Introduction of malicious or other harmful software.

Users should not view this list as exhaustive or exclusive, behaviours of a similar disruptive, malicious or un-productive nature will be likewise deemed unacceptable.

11. Monitoring And Privacy

The College recognises the need to balance enabling and supporting productive IT access alongside requirements and constraints to maintain data security and privacy. The College maintains general activity logs but does not routinely or pro-actively monitor individual user activity. However in order to;

1. Adhere to legislation,
2. Monitor resource consumption,
3. Diagnose systems problems,
4. Respond to requests from individuals themselves, or
5. To investigate allegations of misuse.

The College retains the right to initiate monitoring, to review or interrogate general activity logs or to retrieve specific or individualised content from any College administered system.

Subject to circumstance, this monitoring or retrieval will require the consent of either the Director of IT or the Director of OD & HR.

12. Content Filtering

The College utilises automated systems to prevent or manage access to information or data it considers unsuitable. These controls which can vary by location or function reflect the College's position on what it deems to be acceptable use of its IT resources. The aim of managing some access in this way is to protect both the operation and reputation of the College and to ensure the online safety and security of users, particularly the younger or more vulnerable members of the College community for whom the College has a particular duty of care.

The College actively supports the **UK Safer Internet Campaign** for the safe and responsible use of technology.

13. Policy Application

Users of the College's IT resources have a responsibility to observe and abide by the terms of this policy. In most cases it is likely the College will simply inform a user that he/she is in breach of policy, advise on appropriate corrective action and seek a means to ensure that the unacceptable use or behaviour has ceased.

For staff this contact and guidance is likely to come via the departmental line management, via IT.

For students this contact and guidance is likely to come via a member of the course team, a member of IT or another member of College staff with responsibility for the correct operation of a College system.

The College will respond to repeated or more serious breaches in this policy by invoking the current and appropriate conduct and discipline procedures in force. The relevant policies for staff and students can be found on the staff and student intranets.

14. Legislation

Any breach of existing UK legislation or EU directive covering the operation or administration of the College's IT resources will be considered a breach of this policy.

Equality Impact Assessment

Name of policy/procedure/decision: Policy on Acceptable Use of IT

Provide a brief summary of the aims of the policy/procedure/decision and main activities: This Policy aims to encourage the responsible use of Information Technology [IT] by and for all of its stakeholders. It should reduce the likelihood of legal liability for the College or its IT users, as well as reducing the likelihood of any breach in security practices or regulations that could jeopardise the business and commercial reputation of the College.

Assessed By:	Clare Fraser	**Date:**	17 September 2015

This stage establishes whether a policy, procedure or decision will have a differential impact <u>from an equality perspective</u> on people who share protected characteristics or whether it is "equality neutral" (i.e. have no effect either positive or negative).

The protected characteristics are: age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex and sexual orientation.

1. Who will benefit from this (students/staff/stakeholders)? Is there likely to be a positive impact on people who share protected characteristics, and if so, how? <u>Or</u> is it clear at this stage that it will be equality "neutral"? i.e. will not have a differential impact on any equality group/s? All stakeholders should benefit from this Policy. Acceptable IT use has a range of positive impacts, including access to a variety of learning resources, anytime/anywhere learning, and swift communication. There are particular benefits detailed within this Policy for people who share protected characteristics. Automatic access for all students and staff can assist those with who face barriers in visiting the College, e.g. due to a disability, or having caring responsibilities at home. The Policy states that during periods away from College, e.g. on maternity leave/long term sick, the user account permissions will be adapted to permit access to online communication and information resources. The Policy clearly sets out a commitment to the College's zero tolerance approach to harassment or bullying by stating that offensive, obscene or indecent material will be deemed as unacceptable use.

2. Is there likely to be an adverse impact on people who share protected characteristics? If so, who may be affected and why? Or is it clear at this stage that it will be equality "neutral"?

It is submitted that there is no likelihood that this Policy will adversely affect people who share protected characteristics.

3. What action will you take to ensure that you are monitoring the impact of this Procedure?

Any complaints regarding the implementation of this Policy will be monitored. Equality data will also be monitored in the event that the implementation of this Policy results in the application of disciplinary/conduct proceedings.