ICT Acceptable Use Policy

Version Number	One
Status	Approved
Approval Date: first version	12 January 2015
Approval date: current version	12 January 2015
Responsible for policy:	Vice Principal – Finance
Responsible for implementation:	Vice Principal – Finance
Date of last review:	December 2014
Date of next review:	February 2016
Equality Impact Assessed	Yes
Committee Approval	JCC – 5 December 2014

Table of Contents:

1.0 Purpose 2
2.0 Scope 2
3.0 The College Electronic Mail Service 3
4.0 The College Data Storage Service 3
5.0 User Conduct - Unacceptable Use of the System 3
5.1. Contractual Communications 3
5.2 Unacceptable Use 4
5.3 Exemptions 5
5.4 Electronic Communications – Unacceptable Use 5
5.5 Use of Microsoft OneDrive 6
5.6 Copyright Notice 6
6.0 General Use and Ownership 6
6.1 Confidentiality and Monitoring 6
6.2 Backups 7
6.3 Monitoring 7
6.4 Personal Use and Privacy 7
6.5 Security 8
6.5.1 Confidentiality 8
6.5.2 Passwords 8
6.5.3 Secure PC 8
6.5.4 Access to Facilities 8
6.5.5 Posting/mailings from a College Email Address 8
6.5.6 Threat Management Software 8
6.5.7 Exposure to Unnecessary Risk 9
6.6 Discipline 9
6.7 Modifications 9
6.8 Termination of Use 9
6.9 Exclusions and Limitations 10
7.0 Modifications 10
8.0 Other Relevant Policies and Procedures 10
User Undertaking 11
Appendix One: Examples of Reports Generated From Automated Monitoring Of Network Usage 12
Appendix Two: Reasonable and Unacceptable Personal Use Guidelines 13

1.0 Purpose

The purpose of this policy is to set out the conditions of acceptable use of any and all computer and network related equipment and services owned or used by or with the permission of the College. This provision is referred to in this document as “the System”.

This policy is in place to:

- protect the users of the System, the College and third parties; and
- ensure that scarce resources (machines and bandwidth etc.) are available when needed by authorised users of the system.

Inappropriate use of the System not only exposes the College to risks including the risk of being infected by a computer virus or other electronic threats, the risk that the security of the System and its services may be compromised and the risk that the College might attract legal liability, but also takes up scarce resources.

With the rapidly changing nature of electronic media, and the “netiquette” which is developing among users of external on-line services and the internet, this policy, whilst providing guidance regarding what is and is not acceptable use of the System by users, cannot lay down rules to cover every possible situation. Instead, it expresses the College philosophy and sets forth general principles which should be clear to users in any given situation whether or not their intended use of the System would be deemed acceptable.

This policy should be read in conjunction with other College Policies as detailed in section 8.0.

2.0 Scope

Except for the conditions and users set out in section 5.3 Exemptions, this policy applies to all users accessing the System, including members of staff, contractors or consultants appointed by the College, agency personnel, workers of any affiliates or any other third party, students and anyone else who makes use of the System. This policy also applies to any use whatsoever made of any information technology equipment that is owned or leased by the College, whether such use takes place on College premises or elsewhere (e.g. Outreach centres) and whether or not directly or remotely connected to the System or its networks.

The College connects to the Internet through JANET and is obliged to comply with their Acceptable Use Policy. In addition, users must take care to adhere to appropriate use policies, terms and conditions that may be stipulated by other providers on the Internet or as a condition to using a service.

Many members of the College community will use electronic mail (email) in their day-to-day activities associated with the College business. This policy is designed to inform users of acceptable use and that users should ensure that their use of the System is consistent with other College policies as detailed in section 8.0.

All users of the System should be aware that legal responsibility for email and internet misuse rests with both the College and the individual user. Under the law of defamation, the College may be liable to third parties as the publisher of defamatory or libellous material distributed by any user for whom the College is legally responsible. It is for this reason, that the College has an interest in ensuring that the System is not misused or used inappropriately.

3.0 The College Electronic Mail Service

The email service is provided to send and receive electronic mail via the Internet, using the College email service on the College network for purposes relevant to users' work activities or course of study in order to communicate both outwith and within the College.

The College reserves the right to vary any limits associated with email storage areas in accordance with specific user requirements and, where necessary, will keep users informed. Such limits may be by reference to the physical amount of space available, the number of electronic mail messages held, the size of any attachments sent or any other method the College specifies. The College reserves the right to refuse to accept material, which would exceed any storage limit, and / or to delete material, which exceeds the relevant storage limit.

This service is provided to users without charge as long as the service is accessed via the College network. Remote access (e.g. from home) means that users may incur charges from their own ISP whilst using the service for which they are solely liable. Users should be aware that such use must still comply with the network ICT Acceptable Use Policy.

4.0 The College Data Storage Service

The College will provide users with storage space for data in a format most appropriate to the delivery of ICT services and facilities. In addition, users may have access to discretionary collaborative areas for data which should be shared.

The College reserves the right to vary any limits associated with these storage areas in accordance with specific user requirements and, where necessary, will keep users informed. Such limits may be by reference to the physical amount of space available or any other method the College specifies. The College reserves the right to refuse to accept material, which would exceed any storage limit, and / or to delete material, which exceeds the relevant storage limit.

This service is provided to users without charge as long as the service is accessed via the College network. Remote access (e.g. from home) means that users may incur charges whilst using the service for which they are solely liable. Users should be aware that such use must still comply with the network ICT Acceptable Use Policy.

Only business related data should be stored in the provided data storage areas. Files such as MP3s, Exe, MDB, JPEG (JPG), AVI for example (this list is not exhaustive) should not be stored on College servers unless they are a proven legitimate part of College business. Storage of files such as those aforementioned can have legal implications under copyright and licensing laws.

5.0 User Conduct - Unacceptable Use of the System

5.1. Contractual Communications

Users should, at all times, exercise a general duty of care with respect to the drafting of emails; insofar as emails sent for or on behalf of the College have the potential to place the reputation and business interests of the College at risk by the careless use or abuse of email by users. Email is a competent means of creating a contract; consequently, any user sending an email or digitally signing

a document transmitted by email on behalf of the College must be aware that by so doing, the email or the document may effectively bind the College in contract, even where that was not the intention of the sender.

All business records such as emails forming part of contracts, contracts, agreements, financial statements or other records and any correspondence connected with any legal proceedings should be retained as hard copy on file for a period of at least seven years as these may be needed for legal, regulatory, tax, contractual, audit and evidentiary purposes.

5.2 Unacceptable Use

Under no circumstances is any user authorised to engage in any illegal activity while utilising the College resources.

The following list provides guidance as to which activities constitute unacceptable use of the System. The list is illustrative only and is not exhaustive.

1. Breaching or infringing the intellectual property rights of any third party including but not limited to the installation or distribution of unlicenced software products.

2. The unauthorised copying of copyright materials including digitisation and distribution of photographs from magazines, books or any other copyright sources.

3. Introducing malicious programs into the network infrastructure (e.g. viruses, worms, Trojans, email bombs or malware of any description).

4. Revealing account details or passwords to, or allowing use of a user's account by, others.

5. Using the identity and password of another user for any reason other than a job related function.

6. Using the System or any College equipment to procure or transmit material that constitutes a breach of the Equality and Diversity Policy or the Bullying and Personal Harassment Policy and Procedure, or could be seen as an act of harassment on the grounds of age, gender or gender identity (transgender, transsexual), true or perceived sexual orientation (lesbian, gay, bisexual or heterosexual), marital / civil partnership status, race, ethnic or national origin, disability or religious belief.

7. Accessing, creating, downloading, sending, sharing, storing, printing and / or displaying any offensive, obscene, indecent, degrading or menacing images, data or material from sites containing pornographic or potentially offensive materials that could be considered, by a reasonable person, to be obscene, racist, sexist, or otherwise offensive when viewed or accessed by a third party or creates an unpleasant environment is strictly prohibited.

8. Making fraudulent offers of products, items or services through the use of any College user account.

9. Effecting security breaches or disruptions to network communication whether on the System or on any third party system. Security breaches include but are not limited to, the accessing of data of which the user is not

an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. 'Disruption' may include, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited, see section 5.3 Exemptions.

11. Executing any form of network monitoring which will intercept data not intended for the user's computer.

12. Circumventing user authentication or security of any host, network or account.

13. Using any program / script / command for sending messages of any kind with the intent to interfere with or disable a user's terminal session or the services of any server.

14. Storing on College ICT equipment of data / materials subject to legal or copyright laws, e.g. MP3s.

15. You are responsible for providing proof of the legality of any data / material you store on College ICT Equipment which is required for business use. Ultimately, the College is responsible for the System and reserves the right to remove data when necessary.

5.3 Exemptions

Certain categories of users may be exempted from any or all of these restrictions during the course of their legitimate job responsibilities or approved Studies in a controlled environment and in consultation with the College ICT Services. Providing any data / materials used does not breach copyright or software licencing laws.

5.4 Electronic Communications – Unacceptable Use

The following list provides guidance as to which activities constitute unacceptable use of the System for email and communications. The list is illustrative only and is not exhaustive.

1. Sending any emails which are known to have viruses contained within them.

2. Sending messages of an offensive, bullying, threatening or harassing nature or which contravene the provisions of section 5 (above).

3. Sending unsolicited email messages, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.

4. Subscribing to email newsletters other than for business purposes.

5. Playing online internet games or using streaming media for news, sports scores or other non-business-related real time data streaming. There are specific exceptions for officially approved activities e.g. as part of curriculum delivery.

6. Transmitting by email, retrieving from the internet or storing any communication with obscene language or of an obscene, distasteful, offensive or sexually explicit nature, or which might be judged as such by a reasonable person.

7. Running a business or any commercial activity (other than the business of the College).

8. Misrepresenting the identity of the sender of an email or the source of an email.

9. Intercepting, disrupting or altering electronic communications.

10. Any form of harassment via email, telephone or SMS services.

11. Creating or forwarding 'chain letters' or other pyramid schemes of any type.

12. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.5 Use of Microsoft OneDrive

As part of the student email provision, users are also supplied with a storage area called their **OneDrive** which can be used to store files and data.

Students should be aware that any data stored on their **OneDrive** is subject to monitoring by Microsoft, and any content that is in violation of Microsoft's Code of Conduct is subject to removal and may lead to temporary or permanent shutdown of the account.

5.6 Copyright Notice

College staff and students shall not make, store, transmit or make available unauthorised copies of copyrighted material on the College systems, equipment or storage media.

6.0 General Use and Ownership

6.1 Confidentiality and Monitoring

Whilst the management of the System aims to provide a reasonable level of privacy, users should be aware that the data they create using the System is and remains the property of the College. Because of the need to protect College Systems and also to protect the College from the types of risks mentioned above, the College cannot guarantee the confidentiality of information stored or communicated on the System (including personal storage space on servers). Ultimately the information which is stored on or transmitted via the System is not private to the individual user. Accordingly, users should have no reasonable expectation that personal or commercial information stored or transferred through the use of the System is or shall remain private.

Monitoring of the System will comply with all UK legislation including the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Protection Act 1998 (DPA).

6.2 Backups

All users should be aware that backups are taken at regular intervals for DR&BC purposes and that any data held in either electronic or email format on any of the Servers will be backed up along with all business data and email. Information deleted from the System either deliberately or accidentally can be restored from the backups by ICT Services following a request to do so.

6.3 Monitoring

Members of staff should be aware that the College is permitted to inspect, monitor and / or record any email, internet and storage areas. The College employs a range of monitoring utilities to log information from which it generates reports as illustrated in Appendix One.

The College may also inspect email and storage areas in consultation with a suitable member of the ICT Services, who will log the access and protocols adopted and record the data viewed, in accordance with the provisions of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2006. Specific inspections are carried out where such monitoring reveals the likelihood of risk or inappropriate use. Such inspections extend to both current data and backed up data.

Monitoring or recording may be employed where it helps to:

- prevent or detect crime;
- ascertain whether there are breaches of this or another College policy (e.g. College Security Policy, Personal Use etc.);
- ascertain compliance with any regulatory requirements; and
- maintain or secure the effective operation of the System;

The College may also monitor to ascertain whether a communication relates to College business.

In addition, the College may record or monitor where it is legally obliged to do so. Where appropriate, the College may be required to notify relevant government agencies, the Police or the Scottish Ministers of any incidents of possible concern (e.g. issues of National Security or the accessing of child pornography).

Reports can be made available to the various College Groups and other designated parties as appropriate (e.g. Heads of Department / Managers would be informed if students were downloading inappropriate material for content of study). The Security and IT Asset Management Reports will be confidential to ICT Services and Senior Management Team.

6.4 Personal Use and Privacy

While the College will at all times seek to act appropriately in its use of monitoring, it reserves the right to block sites which are being persistently visited by users which have no legitimate business purpose, where it perceives threat or risk to its business activities or where it infringes the acceptable and personal use policies.

The College will also endeavour to use technical measures to stop misuse as an alternative to monitoring, where it is considered appropriate to do so. However,

users should be aware that, because monitoring is a recognised component of the relationship between the provider of the System and the users, there is no legitimate expectation of privacy when using the System, email, Intranet, Extranet and Internet facilities etc.

On a practical level, members of staff should be aware that, as others may read emails; confidential information should not be sent in this way. For guidance purposes only, examples of reasonable and unacceptable private use are set out in Appendix Two.

6.5 Security

6.5.1 Confidentiality

Access to information contained within the College ICT related systems should be classified as either confidential or not confidential as defined by the College's Data Protection Officer. Examples of confidential information include but are not limited to: company strategies, competitor sensitive information, and student and staff information held on the central records system, specifications, customer lists and research data. Users should take all necessary steps to prevent unauthorised access to this information.

6.5.2 Passwords

Passwords for any College system must be kept secure and not shared. Under no circumstances should users (staff and / or students) disclose their password to anyone. No member of staff should ask for another's (whether staff and / or students') password. To do so would be a breach of the ICT Acceptable Use Policy and disciplinary procedures may be instigated.

All users are responsible for the security of their own passwords and accounts. ALL staff users will be prompted to change their password every 90 days in accordance with the network's security policy.

Passwords should not be written down and on display for all to see. Passwords so discovered will be wiped or removed from display and reported to the relevant authorities.

6.5.3 Secure PC

Users should ensure their computers are secured by logging off when the computer is unattended or by locking the computer when leaving it unattended for a short time as detailed in the ICT Security and Governance Policy.

6.5.4 Access to Facilities

Access to all computer facilities are allowed and enabled once users have completed a valid enrolment process. Students: An SR1 (or other authorised Student Enrolment Form), the issue of a Student ID and Card. Staff by authorisation from HR to ICT Services.

6.5.5 Posting/mailings from a College Email Address

Postings by users from a College email address should contain a disclaimer (this is applied by College email systems by default) stating that the opinions expressed are strictly their own and not necessarily those of the College.

6.5.6 Threat Management Software

All computers which are connected to the College Infrastructure shall run with the Colleges' approved Threat Management Software, which must not be disabled at any time. The only exceptions to this are if ICT Services need to

disable the TM software for technical reasons but all reasonable steps must be taken to ensure the security of the College is not compromised.

6.5.7 Exposure to Unnecessary Risk

Users have a responsibility to ensure that the system is not exposed to any unnecessary risk, and they must use extreme caution when opening email or attachments as they may be “phishing” emails or contain viruses, email bombs, malicious code or other potential risks.

6.6 Discipline

Access to the System is a facility available only to authorised users. As with any other College facility, abuse of these facilities through improper or unacceptable use in breach of this policy or otherwise may lead to disciplinary action.

Students are bound by the College’s Learner Guide: Terms and Conditions and members of staff are bound by the College’s Code of Conduct for Staff. All users of the network are subject to legal compliance with various statutory requirements including but not limited to the Computer Misuse Act 1990, the Copyright, Design & Patents Act 1988, and the Data Protection Act 1998. This includes any upgrades, amendments and any new legislation enacted since the original date.

For the avoidance of doubt, a breach of this policy, and in particular those parts which relate to the processing of personal information, may amount to gross misconduct. In a case where inappropriate use is identified or where such use severely impacts upon the performance or appears to pose a risk to the security of the System or upon College services and facilities, or where such misuse is deemed sufficiently serious, a user’s account may be suspended pending investigation.

6.7 Modifications

The College may from time to time change some or all of the terms of this policy or to modify or discontinue (either temporarily or permanently) the provision of the System. Users will be notified of any such changes where practical. Users do not have to accept such changes, but if they do not, the College shall be entitled to withdraw their access to the System where deemed appropriate. Users agree that the College shall not be liable to them or to any third party for any such change, modification or the withdrawal of access to the System.

On occasion for technical, operational or other reasons, it may also be necessary to terminate services hosted on the System with little or no prior notice. Users agree that the College shall not be liable to them or to any third party for any such termination of such services.

6.8 Termination of Use

Users agree that the College may immediately suspend their use of the System without prior notice for any reason including, but not limited to:

- The College having a reasonable belief that they are or have been in breach of this Policy;
- The College being unable to continue access to the System or any services hosted on the System, due to contractual, economic, technical or operational reasons; or,

- In the event of the College receiving intimation of a user's withdrawal from a course or the termination of employment. In the event of termination, the College will give users such notice of termination as is reasonably practicable.

6.9 Exclusions and Limitations

Access to the System and to services hosted by the College is provided on an "as is" and "as available" basis. No conditions, warranties or other terms are made or given by the College in respect of access to the System. Further, the College can make no guarantee that the services offered on the System will meet users' requirements; that it will be interruption or bug free; timely or ultimately secure.

The College accepts no responsibility for any unintentional deletion or failure to properly store any data or email messages on users' behalf and accepts no responsibility for any costs or damages arising from any interruption, suspension of, withdrawal of or termination of the services on the System.

All users understand and agree that any material and/or data downloaded or otherwise obtained, through remote access and use of or from the System, is done at their own risk and that they will be solely responsible for any damage to their own computer system or for any loss of data that may occur as a result.

The College shall not be liable for any direct, indirect or consequential loss or damages resulting from the use or inability to use the System. These terms and conditions represent the entire agreement between users and the College and supersede any prior agreements, arrangements or representations made by either party relating to access to the System.

7.0 Modifications

The College reserves the right, from time to time change some or all of the terms of this policy or modify or discontinue (either temporarily or permanently) the provision of any systems or equipment. The College will make every effort to inform users of said changes to this policy through the most appropriate means available as soon as is practicable.

8.0 Other Relevant Policies and Procedures

The College has a number of policies and procedures in place which aim to support the conditions for acceptable use of the System. These are regularly reviewed in light of changes in legislation and current good practice:

1. Use of Social Media Policy
2. Equality and Diversity Policy
3. ICT and Information Security Policy
4. Code of Conduct Policy
5. Disciplinary Policy and Procedure

User Undertaking

I have read, understood and agree to abide by and to have my access to and use of the System regulated by the foregoing policy statements.

Signature: …….

Please PRINT name in block capitals ……..

If signed on behalf of a student user please PRINT the student user's name in BLOCK CAPITALS (See note below).

……..

Date: ……..……

[In some instances a parent or legal guardian may be asked to sign where a student user is under 16 years of age, thereby making the parent or guardian responsible for the actions of the student.]

Appendix One: Examples of Reports Generated From Automated Monitoring Of Network Usage

The College uses unobtrusive monitoring software that enables reporting in the following areas:

- **Web Blocker/filter Reports:**
    - Top 20 Report showing the top 20 Domains visited by users
    - Blocked URL Attempts showing users who have attempted to access blocked URLs
- **Content Management:**
    - Inappropriate content report to identify inappropriate content (e.g. Pornography) the location of the file, and the user who created it
    - Scan Report – check for specific categories of files such as MP3s; JPGs; ISOs; MOV; AVI and any other as deemed necessary. This list is not exhaustive and is given as guidance only (which has a major impact on legal liability, copyright and storage capacity)
- **Security Reports:**
    - File Scan for Threats Report showing files posing a danger to network security
    - Threat Alerts which automatically alerts Networks Services when an identifiable threat has been introduced onto any component of the network
- **IT Asset Management:**
    - Installed Software Summary showing all installed software on a particular machine
    - Operating System Summary showing all installed operating systems, serial numbers and service packs
    - Hardware/Software changes showing these changes over a given period
    - Machine Configuration showing an overview of each machine's installed software, hardware and summary of disk usage
- **Email Filter (to block inappropriate content and spam):**
    - Biggest emails sent
    - Largest volume of email sent
    - Most emails received
    - Most email sent
    - SPAM summary

The College routinely generates these and other network activity reports to ensure that users are complying with College policies and procedures and to enable the College to safeguard itself and the System against known and perceived threats, inappropriate or malicious use by users or users deliberately or inadvertently acting in a manner which breaches College policies as detailed in section 8.0.

Appendix Two: Reasonable and Unacceptable Personal Use Guidelines

The following details College policy for users on what is considered to be reasonable personal use and what is considered unacceptable personal use of ICT systems. This is not an exhaustive list. The College takes the view that personal use should be within reason and that it should not be abused to the detriment of an individual's work outputs. Use of the System for personal purposes should therefore be limited to non-working hours.

Acceptable Personal Use	Unacceptable Personal Use
Staff: ▪ Access to sites relevant to curriculum area of team. ▪ Accessing sites of personal interest out with normal working hours or during lunch breaks. ▪ Download of licenced or non-copyright materials relevant to curriculum area of team. ▪ Use of email facilities in course of College duties and responsibilities. ▪ Use of the internet to gain experience of modern business / commerce purposes / practice i.e. Personal email. Internet purchases; online travel bookings / banking (Fife College cannot guarantee the security of credit card information which may be accessible). Students: ▪ Accessing sites which are relevant to course of study and timetabled activities. ▪ Accessing materials relevant to course of study / subject area / timetabled activities. ▪ Use of email facilities relevant to course of study / subject area / timetabled activities in order to facilitate effective communication between classmates.	Staff and Students: ▪ Accessing or downloading materials from sites containing pornographic or potentially offensive images. ▪ Downloading any copyright or unlicenced materials which infringe the law and / or expose the College to risk. ▪ Sending email communications containing offensive, abusive, harassing or threatening language or images. ▪ Use of chat lines. ▪ Forwarding or distributing items of 'junk' via mail facility. ▪ Forwarding of inappropriate material which wastes time. ▪ Storage of non-business-related and personal files and details. ▪ Committing the College to anything which incurs unauthorised cost or any unauthorised subscription to paid for services.