Internet, Network and Digital Communication Policy

POLICY / DOCUMENT PURPOSE STATEMENT

This document outlines guidelines and restrictions that are placed on students and staff relating to the use of digital communications, the internet, and the college network (LAN\WI-FI). It is also designed to ensure that all employees, governors, and learners achieve and maintain acceptable standards of performance with these systems.

APPLICATION

The policy applies to all individuals accessing the college network, services, and data held within.

INTERPRETATION

Further guidance on the use or interpretation of this policy may be obtained from the IT department.

LINKS WITH OTHER POLICIES / DOCUMENTS

Fircroft IT User Agreement,
Staff Disciplinary Policy & Procedure,
Code of Professional Standards,
IT Security Policy,
BYOD Policy,
Call Logging & Escalation Policy

Version number	3
Owner / Department	Andy Gazey/IT
Date of implementation	12/01/2022
Review date	09/02/2024
Ratified / Authorised by	09/02/2022 (Operations Committee)
Equality Impact completed	12/01/2022

1. Introduction

1.1. The provision and use of E-Mail and the Internet in the College opens up opportunities for collaboration, communication, and research, but it may also create unforeseen consequences and problems. E-Mail can boost efficiency through improved communication, and internet use may stimulate creativity; facilitate research and the gathering of information, however, both can also offer opportunities for misuse.

1.2. It is important that College Governors, staff & students are aware of the guidelines that they are expected to follow in using E-Mail, the Internet, and the college network. The College's policy is set out below to ensure that users understand how the system should be used. In this policy, users are made aware of the possible dangers of using the systems and the fact that disciplinary action may result from its misuse.

1.3. The policy attempts to achieve a balance between allowing users access to E-Mail, Internet, and network services to assist in their work and studies whilst addressing, as far as possible, the risks of such access.

1.4. It is therefore essential that users read and agree to be bound by these guidelines and make themselves aware of the potential legal liabilities involved in using E-Mail, the Internet, and networks.

2. General Points

2.1. Use of E-Mail, the Internet, and the college network is primarily for work or study-related purposes.

2.2. The College is the owner of digital and Internet communication resources. These are designed to assist in the performance of work and studies. Users should, therefore, have no expectation of privacy in any communications sent or received, whether it is of a business/course related or a personal nature, and in view of the range of legal liabilities that can arise from users having access to communication services and the Internet, the College may monitor and intercept communications as considered necessary within legislative requirements.

2.3. Any user has the right to request to see certain information, commonly referred to as a subject access request. This right is created by section 7 of the Data Protection Act (2018). Students and staff may request to see a copy of the information the college holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee will be entitled to be: told whether any personal data is being processed, given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people; given a copy of the information comprising the data; and given details of the source of the data (where this is available).

2.4. The College accepts that there are occasions when Governors, staff, and students will receive unsolicited material of an obscene or offensive nature. However, you should note that under this procedure improper use of digital communication, the Internet, and the college network by users to knowingly access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist, or defamatory could, in certain circumstances, be treated by the College as gross misconduct, or result

in students being excluded from their course, or from the College. The College reserves the right to use the content of any communication in any disciplinary process.

2.5. All College Microsoft applications and data held within are protected by enforced Multi-factor authentication. This is to protect access to College applications and data in the event of a password breach. Should a user suspect a password breach, users must contact IT support immediately so that all logins can be forcibly logged out and a new password given.

3. Use of Digital communication\Email

3.1. E-Mails and Digital Communications should be drafted with care. Due to the nature of digital communication, it is easy to forget that it is a permanent form of written communication, and that contents can be recovered even when it is deleted from your computer. As such users must take reasonable care in ensuring that all digital communications are constructed so as not to cause annoyance, inconvenience, or needless anxiety.

3.2. Users should not make defamatory remarks in communications about governors, staff, students, competitors, other stakeholders, or any other person since written derogatory remarks can constitute libel.

3.3. Sharing of personal or confidential information is prohibited unless formal approval has been granted by the college. Sharing of personal or confidential information should be done through approved secure channels, such as Microsoft OneDrive, any insecure third-party applications must never be used to share such information.

3.4. Any group E-mail addresses **must not** be used for personal reasons (e.g. personal events, sale of goods, personal or political views),

3.5. By sending digital communications on the College's systems, you are consenting to the processing of any personal data contained in that communication and are explicitly consenting to the processing of any sensitive personal data contained within.

3.6. Any group E-mail addresses are for internal use only and must not be given to third parties.

3.7. Be security conscious. The Data Protection Act requires that adequate security is maintained to protect personal information held on e-mails, related archives and software **(see appendix 1).** Do not allow anyone to use your network log-on and password, and do not leave your network account logged on when you have walked away from the computer without ensuring you have locked the computer to prevent others from accessing your account. Please see the colleges IT Security Policy for further information.

3.8. Email usage is permitted on personal devices (such as smartphones), which will be protected using enforced multi-factor authentication. All devices should utilise access security such as a strong password or biometric security. Should users need help setting up email on a personal device, please contact IT-Support for assistance.

3.9. We receive a large number of targeted phishing attacks across the sector. If you do receive a suspicious email, do not open the email, reply to the email, enter any details, or click any links within. All suspicious emails should be immediately reported to IT-Support. Please see Appendix 4 for further advice on Phishing emails.

3.10. When an employee/governor leaves the College's employment, an E-Mail will be generated from H.R. to I.T. who will then disable (*not delete*) the account with immediate effect and forcibly log out all sessions. (*unless instructed differently by the leaver's line Manager*).

3.11. When a student leaves the College at the end of their course their account will be disabled two calendar weeks after the official course end date. Where a student has their enrolment terminated prior to the course end date, the I.T. Dept will disable the account with immediate effect (*This will initially be confirmed in an E-Mail to IT Services from Curriculum/Admissions*).

3.12. All digital communications sent to accounts using the fircroft.ac.uk after a user account has been disabled will be returned to the sender. Where I.T. have been requested to keep the account open due to the sharing of information, and legal/financial data then confirmation by E-Mail will be required from the relevant Senior Manager. After a period of three (3) months, all remaining Emails relating to the former user will be deleted.

4. Use of the Internet

4.1. Computer and internet access is provided to all users on the understanding that it will be exercised in a responsible manner, for educational purposes and College business use.

4.2. All sites accessed by users must comply with the restrictions set out in these guidelines. The creation or transmission (*other than for properly supervised and lawful research*) of any offensive, obscene or indecent images, data or other material may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct, or result in a student's exclusion from their course and/or the College.

4.3. Copyright applies to all text, pictures, video, and sound, including those sent by E-Mail or on the Internet. Files containing such copyright-protected material may not be downloaded, forwarded, or transmitted to third parties without the permission of the author of the material or an acknowledgment of the original source of the material, as appropriate.

4.4. Copyrighted material must never be downloaded/uploaded without the clear consent of the copyright holder. It is the responsibility of the person downloading/uploading the material to ensure no copyright is infringed.

4.5. Users must not use the internet in a way that denies access to others, for example by deliberate or reckless overloading of College systems.

4.6. Users should not upload unknown data onto the College's systems without having them scanned for viruses.

4.7. All internet traffic from a person's account\devices across the college network will be monitored and recorded, and may be used for investigative reasons if required.

5. Use of the College Network

5.1. Fircroft College's IT system and network (including WI-FI) are provided by JANET, government-provided network for the educational community. Staff, students, and governors must adhere to the 'JANET Acceptable Use Policy' (Appendix 2). This includes

(but is not exclusive to): Transmitting any offensive, obscene or indecent images, data, or slanderous material. Anything designed or likely to cause annoyance or inconvenience. Anything that infringes the copyright of another person. Commercial or advertising material. Viruses that corrupt and destroy data, or that violate the privacy of the network. Anything that could be deemed as promoting radical material relating to subjects of terrorism/extremism.

5.2. Fircroft also has a duty to comply with all statutory responsibilities laid down in relevant legislation and guidance relating to the use and control of Information Technology including, but not limited to: Data Protection Act (1998), Counter-Terrorism and Security Act 2015, Regulation of Investigative Powers Act (2000), Freedom of Information Act (2000), Human Rights Act (1998), Computer Misuse Act (1990), PREVENT Duty guidance (2015).

5.3. To meet the above objectives effectively, Fircroft's IT systems filter or block certain network traffic and content that poses risks, and all traffic across the college network will be monitored and recorded.

6. Use of Office 365 & Other Collaborative Tools

6.1. The college's continued digital approach means that staff and students are now able to access the college's Office 365 platform and its supporting applications (SharePoint, Teams etc). It is expected that collaborative tools will become more widely used and accessible. The college requires that users follow the same guidelines outlined in section 4 of this policy.

7. General Computer & Laptop Usage

7.1. Users are responsible for safeguarding their password for the system. For reasons of security, passwords should not be printed, stored online or given to others. User password rights given to users should not give rise to an expectation of privacy. Should you suspect a password breach, you must contact IT support immediately so that all logins can be forcibly logged out and a new password given. Please consult the Fircroft IT Security policy for information on securing Fircroft and associated accounts.

7.2. Users' ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Users should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

7.3. IT devices are loaned to users and students for the sole use of work or study. When loaning IT equipment for the purpose of work or study, a loan agreement must be signed and all conditions in the agreement accepted **(See Appendix 3).** The loaned IT equipment remains the property of Fircroft College and must be returned to the College within the timescales accepted in the agreement or when requested to do so by the College.

7.4. Loaned IT equipment is for the sole use of the person on the loan agreement form and must never be given to another person for use.

8. I.T. Support

8.1. IT Support is there to assist you. If you require any information or help about the use or set up of your College computer you should contact IT by email ITSupport@fircroft.ac.uk

9. Misuse of Digital Communications, Internet, or the College Network

9.1. The digital systems, Internet, and network facilities provided by the College are provided on the understanding that users will use them in a responsible manner. However, misuses such as excessive private use of the E-Mail system during working hours or excessive private access to the Internet during working hours, or knowingly viewing or downloading improper or obscene materials may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct, or result in a student's exclusion from their course and/or the College.

9.2. If the College considers that a user is abusing the College's policy it reserves the right to withdraw any of the facilities provided by any member of staff or student and escalate the matter to the disciplinary process where needed.

9.3. Use of the College systems, Internet, and network will signify that a user has read and understood the above guidelines and has agreed to comply with these guidelines at all times.

10. PREVENT Agenda

10.1. In order to safeguard students utilising the IT facilities at the College and prevent individuals from accessing extremist materials via the College's network, we will ensure:

10.2. The organisation will retain the ability to log and retain records of all electronic communications (web browsing, e-mail traffic, etc.) by users on the College network.

10.3. Appropriate staff will be available to monitor any aspects of its telephony network, including mobile phones and any computing facilities made available to staff, students, and visitors.

10.4. Only College approved software will be supported by the College and allowed to be used on the College network.

10.5. Any unauthorised software that breaches College policies and/or presents a risk to staff/student safety will be removed and appropriate action taken where necessary.

10.6. All unusual and/or suspicious events including breaches of security are to be reported immediately via the safeguarding team for further investigation.

Appendix 1

Data Protection Issues

Personal data is subject to the Data Protection Act 2018. Under the terms of the Act, personal data includes any information about a living identifiable individual, including their name, address, phone number, e-mail address and any other information about the individual. If you include such information in an e-mail, you are deemed to be processing personal data and must abide by the law. In particular, you must not collect such information without the individual knowing you propose to do this; you may not disclose or amend such information except in accordance with the purpose for which the information was collected; and you must ensure the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her on the e-mail system, or held in separate archives of e-mails. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by inaccurate information.

The law also imposes rules on the storage of personal data. Such data should only be kept for as long as it is needed for the purpose for which it was collected. If you maintain your own stores of emails, you should ensure that such stores are not maintained for longer than is necessary for the purpose for which it was collected. E-mails should be held in such a way that they can be easily identified, reviewed and, when necessary, destroyed.

Finally, the law imposes strict rules on the transfer of personal data outside the European Economic Area (EEA). Transfer is not just the deliberate sending of information outside the EEA, but also allowing third parties from outside the EEA access to the personal data held in the UK.

Therefore, you should not:

- Use e-mails for any purpose that is not permitted under the College's notification under the Data Protection Act;
- Use a false identity in e-mails you send out;
- Exploit mail servers or other systems to facilitate the widespread distribution of unsolicited and unwanted e-mails;
- Use e-mails for communicating confidential or sensitive matters relating to individuals;
- Obtain, handle or disclose personal information without ensuring you are complying with the law or
  with the College's notification to the Data Protection Commissioner;
- Allow third parties to read personal information in e-mails or attachments by leaving your screen in view of such third parties;
- Create or forward advertisements, chain letters or unsolicited e-mails;
- Read other peoples' e-mails sent to someone else without their express permission;
- Pass on your password or ID to any third party;
- Invade someone's privacy by any means using e-mail;

- Send e-mails containing personal information outside the EEA, or allow third parties outside the EEA to read your e-mails containing such information without checking with the College's Data Controller.

You should:

- Be cautious about putting personal information in the body of the text, especially if it is of a sensitive or confidential nature;

- Comply with a request from the Data Controller, your manager or a member of the Senior Leadership Team to inspect your e-mail archives and/or to print out items relevant to a particular individual if that individual demands a copy of his/her file. This will only be requested when required under the Act, or where there is good reason to believe that violations of the law or of College policies have taken place, or for some other compelling or time critical reasons;

- Agree to pass to the College all of your e-mail records if you leave the employment of the College;

Note that the recipients of your e-mails, the originators of e-mails you receive and the content of all emails sent or received may be the subject of scrutiny within current legislative provision.

Appendix 2 Janet Acceptable Use Policy

1. The Janet Network ("Janet") is the communications network operated by Jisc Services Ltd (Jisc) to serve UK education, research and other public sector purposes. Its primary purpose is to enable organisations in these communities to fulfil their missions of providing education, research, of supporting innovation, and of civic engagement more widely.

2. This Acceptable Use Policy applies to two broad categories of organisation: those connecting directly to Janet in their own right ("Connected Organisation"); and those connecting indirectly, as a partner to the directly-connected organisation and with the connection made through the latter organisation's own connection(s) to Janet ("Partner Organisation"). It also covers the granting of access to Janet to guests visiting an organisation with a Janet connection. In conjunction with MF-POL-007 the Janet Security Policy, it is an integral part of GEN-DOC-009 the Terms for Provision of the Janet Service (Janet Terms)[1].

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 MF-POL-053 the Janet Network Connection 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 Network Connection Policy.

4. Copies of the Janet Terms, the Janet Network Connection Policy and the Janet Security Policy may be found at ji.sc/policies.

5. Connected Organisations and their Partner Organisations may use Janet for the purpose of communicating with other Connected Organisations, 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 Connected Organisation for any lawful activity in furtherance of the missions of the Connected Organisation. Use by the Connected Organisation 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 Connected Organisation to ensure that its users (and their Partner Organisations) use Janet services in accordance with the Acceptable Use Policy, and with current legislation. (See Note 2)

8. Janet may not be used by a Connected Organisation, Partner Organisation or their users 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 or 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 Jisc resources, including time on end systems on another Connected 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 Connected 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, malware, ransomware or other harmful software via Janet to resources on Janet, or on another Connected Organisation's network.

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 Jisc will also be regarded prima facie as unacceptable use of Janet.

19. It is the responsibility of the Connected Organisation to take reasonable steps to ensure its users, Partner Organisations and their users comply 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 users of the Connected Organisation with access to Janet of their obligations in this respect (see Note 7).

20. Where necessary, service may be withdrawn from the Connected 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.

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 Connected Organisation, other than this is acceptable where lawful. However, it should be noted that there are legal constraints applying to a publicly funded Connected Organisation in such activities. Where the Connected 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 Network Connection Policy.

Note 2: It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of Janet on the part of its users and appropriate disciplinary measures taken by their Connected 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 Connected 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 Connected Organisation or by Jisc. For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.

Note 6: Where a Connected 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 Connected Organisation, will not be a breach of clause 15. However, the User Organisation should inform Jisc 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 Jisc CSIRT in investigating the perceived attack on the Connected Organisation, or automatically blocking it. Jisc CSIRT should be contacted via the details at https://www.jisc.ac.uk/csirt.

Note 7: In order to discharge this responsibility, it is recommended that each Connected Organisation establishes its own statement of acceptable use within the context of the services provided to its users. 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.

Appendix 3

Loan IT device agreement

The loan IT agreement exists between Fircroft College and the named person who will sign the IT loan device agreement.

If a person wishes to borrow IT equipment, the agreement must be signed and dated to confirm that the conditions set out are agreed to. These conditions are that:

- The computer will be loaned to the named person for the duration outlined in the agreement, and must be returned within 5 working days from the end of the agreement date, or when requested to do so by Fircroft College. Failure to return the device above in the specified timeframe will result in the College proceeding with a reclaims process.

- The IT equipment outlined above will remain the property of Fircroft College, and is loaned for the sole use of assisting you with your work or studies.

- You understand that in the event of a loss involving a laptop computer that the insurer will impose an excess of £1000 for which you will be personally liable.

- You will take all reasonable steps to ensure that the computer is not damaged, lost or stolen while in your care and custody.

- If the IT equipment outlined above is lost or stolen, you will report this promptly to the police and obtain a crime reference number, which you give as soon as possible to the College for insurance purposes.

- Reasonable health and safety precautions should be taken when using a computer. The College is not responsible for any damage to person or property resulting from the computer or equipment loaned.

- If the IT equipment outlined above is damaged, lost or stolen that you will report this promptly to colleges IT Manager.

- You will not lend the IT equipment to any other person.

- You will not install any software without the permission of the Colleges IT Manager, and you will not attempt to make any changes to the inner hardware of the device.

- The computer and the connectivity equipment must not be used for any illegal and/or antisocial purpose.

- There may be occasions when we need you to return the computer to the College for upgrades and maintenance. It is your responsibility to return the computer to the College if\when asked to do so.

- Fircroft College cannot be held responsible for the loss or damage of any data on the computer.

- Should you move address from the location you have given us, or your contact details change, it is essential that you inform the College at the earliest opportunity.

- When returning the device to the college, all personal data, including any saved passwords or accounts must be removed.

Appendix 4

IT induction - Phishing email template

As you may know, we receive a large number of phishing attacks across the sector.

We have also had an external organisation hacked, which has led to phishing emails being sent to users on their marketing list from their own, corporate account.

The simple advice remains to be very cautious when opening unexpected emails, or emails that are asking you to do something unusual, for example, clicking a link to open an unexpected voicemail message.

Whilst most scam emails are easy to spot, some are very sophisticated and personalised, and can look very genuine.

If you do receive a suspicious email, please let us know so we can add the sender to our blocked list.

Below is a quick video on phishing emails.

https://www.youtube.com/watch?v=XsOWczwRVuc

Also, google have a phishing quiz to try out your phishing skills over a coffee.

https://phishingquiz.withgoogle.com/

Below is a website where you can check if your email address has been compromised (you can use this for personal email addresses also).

https://haveibeenpwned.com/

I have also linked below some slides from the security awareness training we held last year.

Security training

As always, any concerns, questions, etc, please do not hesitate to contact IT-Support.