KIRKLEES COLLEGE

Information Security Policy

September 2019

Kirklees College – Information Security Policy

Introduction

This policy is regulated and updated by the Directorate of Information Technology (IT). It is available to all users of Kirklees College IT services. It will be reviewed and updated on a regular basis to reflect changes in technology and the way in which systems are used, it may also reflect new developments within the IT infrastructure.

The key goal of the Kirklees College Information Security Policy is to present the standards and guidelines that will preserve the confidentiality, integrity, and availability of information and data within the College and with partner organisations. These are core principles within the field of information security and in line with legislation regarding the protection of individual rights. Further detail is provided below;

Lawful Basis for Processing – all data collected, processed and shared by the college should only relate to the performance of the business relationship.

Confidentiality - Data is only accessed, processed and shared by authorised users and organisations.

Integrity - Data will be accurate, authentic, complete and processed correctly. Where necessary personal data will be removed at the owner's request where this does not impact on the business of the college.

Availability - Data can be accessed when required, by those who are authorised to access the data. Data subjects will have access to personal data upon request as stipulated by the General Data Protection Regulation (GDPR) under the section Individual Rights.

Data Breaches – any breach of the GDPR should be reported to the designated Data Protection Officer who will assess the breach and advise on any appropriate action. Individuals whose data may have been compromised will be informed in a timely manner in line with GDPR recommendations.

The policy will help the College to maintain the above principles and mitigate the threat of any potential security breaches.

1. Purpose

The purpose of this policy is to detail the standards and guidelines that users should adhere to when accessing the facilities of Kirklees College. It also defines procedures that will be taken to assist in providing a secure environment for information accessibility. Finally, it provides further information, clarification and advice in the form of an 'advisories' section at the end of the policy.

In summary, this policy will provide a framework for protecting;

i. The IT facilities
ii. Data and information stored both internally and externally
iii. Users of the IT facilities

2. Scope of the Policy

The Information Security Policy applies to the use of the IT facilities, electronic and paper based systems provided and managed by Kirklees College. The Policy is applicable to all users of these facilities. This includes (without exception) staff members, students, governors and visitors, including contractors and temporary workers.

3. Standards of Acceptable Use

Users are permitted and encouraged to use the IT facilities on condition that the use is appropriate and proper and is in line with the intended college business functions. It is a condition of use of the facilities that a staff member, student or authorised person agrees to be bound by the relevant policies and regulations. The College policy 'Acceptable use of IT systems for staff and students' provides further detailed guidance on IT usage. Users are also advised to read and comply with the JANET Acceptable Use Policy (http://www.ja.net/company/policies/aup.html) and JANET Security Policy (http://www.ja.net/documents/publications/policy/security.pdf).

The following standards must always be followed at all times, when using the IT facilities;

3.1 General Standards – Security policy

1. Use of the IT facilities must comply within the law at all times.

2. Users must not view, store or distribute any materials which are deemed contrary to the UK Governments Prevent agenda.

3. Users must not attempt to circumvent, jeopardise, damage or destroy the security procedures and measures that exist within the IT systems and facilities.

4. Users must not access, run, distribute, copy, store or install any software which is illegally licensed, is unlicensed, or has not been specifically authorised for your use.

5. Users must not use the IT facilities to harass, slander, libel, defame, intimidate, impersonate, abuse or cause offence to other users.

6. Users must not use the IT facilities for the creation, communication, storage, download or displaying of any obscene, offensive, defamatory or indecent images, material or data.

7. Users must not use the IT facilities to conduct any form of commercial activity for personal use.

8. Users are not entitled to use a computer that they have not been authorised to use.

9. Use of the IT facilities must not be used to commit any form of fraud, piracy or unauthorised use of data; specifically (but not restricted to) copyrighted material and intellectual property of third parties.

10. Users must not attempt to bypass the restrictions placed on PC's, for example this may include the use of unauthorised games or software, run from a CD or USB device.

11. Users must not interfere with the normal operation of the IT facilities. Examples of this would include the propagation of computer viruses, or sustaining a high volume of network traffic which may disrupt the normal operation of the network.

12. Users must not attempt any unauthorised access to a remote system.

13. The use of hacking techniques of any form is strictly prohibited within Kirklees College IT facilities. This can include (but is not limited to) port scans, denial of service, monitoring, address spoofing and network flooding activities.

14. Users must not apply any steganography (hidden data) or covert channel techniques upon data or the IT facilities. This includes (but is not restricted to) the unauthorised use of encryption, malicious code, data streams and cryptography.

15. Users must not make any attempt to modify, damage or destroy another user's data.

16. If users are aware of any security breaches affecting yourself or other users then you are responsible for reporting it to the IT Service Desk. The incident will then be logged and passed on for investigation. Examples of activities that could be classed as security incidents include; compromised password, hacking attempt, PC virus infection, missing/deleted computer files, unaccounted for changes to system data and unauthorised users attempting access to facilities.

17. Users should be aware that failure to comply with the standards of this policy may expose the College to serious liability and damage reputation. Kirklees College is committed to responding promptly to any potentially damaging publication and will withdraw any unacceptable materials and taking any appropriate action.

18. User must always lock the computer if leaving their immediate area/desk but remaining logged on (to lock your PC, press control, alt and delete together, or press the Windows key and L)

19. Users must always log out of the computer when the session has finished and close down at the end of the day

20. Information should not be stored for longer than necessary

21. No personal information should be stored on removable media and regular threat scanning should be undertaken on such devices

22. Personal data must not be stored on any mobile device. All personal data should reside on central systems and be accessed securely across encrypted links

23. Staff with a college device should ensure that all necessary precautions are taken when taking equipment offsite to prevent theft. In addition all devices need to be kept up-to-date with anti-malware software and protected by password or a PIN.

3.2 Standards of Email Usage

Users are permitted and encouraged to use the email facilities on condition that that the use is appropriate and proper, and is in line with the intended business functions of the College. Users need to comply with the following regulations;

1. Email is not a secure method of communication. Therefore, sensitive data should not be sent via e-mail, unless the permission of the owner of the data has been obtained. If this has not been obtained and email is the only form of communication that can be used, then encryption techniques must be used to send the email (Please contact the IT Service Desk if you need further assistance).

2. When sending email to multiple external contacts, BCC must be used.

3. Email must not be used for the creation or transmission of material which brings the College into disrepute.

4. Users must not disclose or publicise confidential information which includes (but is not limited to) financial information, databases and the information contained therein, computer network access codes, personal information of staff members or students, and business relationships.

5. Email use must not involve the creation or transmission of obscene, defamatory, abusive, threatening or offensive material, or material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.

6. Users must not open emails (or email attachments) or reply to emails which are unmistakably from unsolicited or non-trusted sources. A suspicious email should either be deleted without opening, or raised with the IT Service Desk for further investigation.

7. Users must not knowingly transmit by email any file attachments which may compromise security. For example, an attachment infected with a virus.

8. Email use must not involve the creation or transmission of copyrighted material or software without prior consent of the author.

9. Email use must not be used for the creation or transmission of any obscene, offensive or indecent images, data, or other material.

10. Email use must not be used for the creation or transmission of unsolicited commercial or advertising material, chain letters, press releases, or any other junk-mail of any kind.

11. Users must be aware that Kirklees College takes no responsibility for users who open spam emails, or are misled by any type of online scam, and ultimately have their personal details compromised. It is entirely the responsibility of the end user to be knowledgeable and aware of such threats and how to avoid them.

12. Email accessed through a personal device such as a phone or tablet are reminded that these devices should be secured with a password or PIN and that no personal or confidential data should be stored on the device.

3.3 Standards of Personal Use of Email

It is acceptable for the College IT facilities and email accounts to be used for personal email, subject to the following limitations;

1. All personal email messages are treated as potential corporate messages of the organisation.

2. All personal email messages represent personal opinions, and not those of the College.

3. Personal email use must not be for any type of personal or financial gain, or for any form of commercial or profit-making nature.

4. It must not be used in a way which competes with the business functions of the College.

5. Personal use must not be connected with any use or application that conflicts with an employee's obligations to the College.

6. Personal use must not be connected to any purpose or application that conflicts with the College's rules, regulations, policies and procedures

7. The College is entitled to redirect email, or disable the email accounts, of staff that have left the organisation. Users are responsible for the future of their personal emails.

8. The distribution of any information through the College infrastructure is subject to scrutiny including blocking the message. The College reserves the right to determine the suitability of this information.

9. Personal use of email should not be excessive and undertaken within the persons own time.

10. Personal email will be subject to the same filtering system in use for business email.

3.4 Standards of Internet Usage

Users are permitted and encouraged to use the IT facilities for Internet access on condition that the use is appropriate and proper, and is in line with the intended business functions of the College. The facilities that are provided must not be used for the following;

1. Internet access must not be used for any action which may be deemed likely to bring the College into disrepute.
2. Internet access must not be used to commit any form of fraud, or be used for the unauthorised copying, storage or distribution of software or copyrighted material.
3. Internet access must not be used for the creation, storage, download or displaying of any obscene, offensive, defamatory or indecent images, material or data.
4. Internet access must not be used to harass, slander, libel, defame, intimidate, impersonate, cause offense, or abuse other users.
5. Internet access must not be used to visit, or attempt to visit, sites that contain obscene, hateful, pornographic, offensive, insulting, derogatory, racist, sexist or otherwise illegal material.
6. Users must not publish defamatory and/or knowingly false material about Kirklees College, or anyone representing Kirklees College (staff member or student) on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
7. Users must not post messages on any website in the public domain, which may be deemed damaging or offensive to any users (staff or student). Examples of this include social networking sites, such as facebook, myspace, bebo, youtube or ratemyprofessor.
8. Users must not reveal confidential information about Kirklees College in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions.
9. Users who have a requirement to access unauthorised material or access an unauthorised website should contact the IT Service Desk.

   See also the Social Networking Guidelines

3.5 Password Standards

Your password is your key protection against your account being compromised. A secure password should prevent security breaches on your account. In order to ensure that both personal and college data remain protected, users are responsible for safeguarding their passwords. To help maintain password security, users will be required to comply with the following password restrictions;

1. Change your password regularly, usually every 60 days.
2. Choose a password of minimum six characters with at least one numeric character (this is enforced by system policy).

3. Users cannot re-use old passwords within 8 change periods.

4. Choose a password that cannot be easily guessed or hacked. For example, avoid using a name, a car registration number, or a football team. It is also advisable to avoid using standard dictionary words.

5. Users must not disclose their password to anyone, or write down their password, where it can be accessed by others.

6. Users must change their password immediately if it is suspected that someone has discovered it.

7. Users are advised not to use the 'Save Password' option in login boxes when browsing on the Internet.

8. Never use the same passwords for sensitive account information. In particular, ensure that your college account passwords are not the same as any online/PC personal accounts

4. Monitoring and Accountability

The College recognises that misuse of the IT facilities could have a damaging effect on other users, and also the reputation of Kirklees College. We are obliged to monitor activity to fulfil our responsibilities with regard to UK law, the Government PREVENT agenda and the JANET Code of Conduct, and therefore, the College will maintain appropriate monitoring and recording arrangements in relation to all IT services. This arrangement will apply to all users and data (including archived data) and all users may be used for investigative purposes. The College will apply the following conditions with regards to monitoring;

1. The College reserves the right to access user accounts and data in the interests of detecting or investigating unauthorised use of the facilities.

2. The College reserves the right to access user accounts and data in the interests of an appropriately authorised investigation – legal or disciplinary.

   Individual use of College IT facilities can be subject to monitoring for security and/or network management reasons. The College is not required to provide individual notice of such monitoring.

3. Any illegal use will be dealt with appropriately. In certain circumstances, access to data may be provided to third parties for example, the Police will have access to recorded data if required.

4. Users are advised that the College may, at its discretion, apply message monitoring, filtering and rejection systems as appropriate.

5. Legal Advisories

The use of College resources is subject to UK law and JANET Code of Conduct. The key areas of law which apply to the use of IT facilities are listed below. Please note this is only a brief summary of some of the legal requirements and outcomes that users should be aware of:

General Data Protection Regulation - The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Data Protection Act 1998 - Users have responsibility and liability if they process personal data. Users must be particularly careful not to disclose personal data to anyone who does not have the right to access it.

Copyright, Design & Patents Act 1988 - Users must not use or copy any software for which there is no software licence. Users must not install any software without authorisation.

Computer Misuse Act 1990 - The following activities are a criminal offence; unauthorised access (hacking), unauthorised access with intent to commit further offence and unauthorised modification (including introducing a virus).

1. Users should be aware that logs of network transactions can be produced as evidence, to assist with the above legal requirements, as part of criminal or civil law proceedings.

2. The processing of information which contains personal data (this includes photographs) about individuals requires the express written consent of those individuals. Use of personal data which does not have this approval will be regarded as an illegal violation of the data protection regulations as monitored by the Information Commissioners' Office.

3. Should a user publish any material which is pornographic, violent or which falls under the Obscene Publications Act 1959, this will be classed as a criminal offence. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.

4. The Internet is within the scope of legislation relating to libel, where a statement or opinion is published, and which adversely affects the reputation of a person, group of people, or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email/author.

5. Material which is discriminatory, or if it encourages discrimination, may be illegal under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995. This may involves discrimination on the grounds of sex, race or disability.

6. Users who attempt to browse to sites which contain illegal, violent, pornographic, obscene or criminal material will be blocked by the College web filtering systems. This activity will be recorded and the logs of this activity investigated and potentially reported to the appropriate authorities.

7. When an account is opened for you and you are provided with access to the College IT systems, you agree to comply with all relevant legislation and regulations.

6. Violation of the Information Security Policy

When a violation of the Information Security Policy has occurred, the College will begin proceedings in accordance with the college disciplinary process. Possible courses of action are detailed below;

1. Instances of non-compliance with the Information Security Policy will be appropriately investigated. Users may be subject to the college disciplinary procedures. Depending of the outcome of any investigation, the end result may ultimately lead to dismissal on the grounds of gross misconduct.

2. The College will investigate complaints received from both internal and external sources, regarding misuse of the College IT and email facilities.

3. The investigation of facts of a technical nature, e.g. to determine the source of an offending email message, will be undertaken by the appropriate internal departments but may involve 3rd party external assistance, if required.

4. Should there be any evidence of a criminal offence having occurred; the issue will be reported to the police. The College will co-operate with the police or any other external organisations who may become involved in the investigation.

5. Any behaviour which may be deemed threatening to others, or serves to harass or intimidate others, may result in disciplinary procedures and/or a criminal investigation.

7. Advisories and General Considerations

Kirklees College aims to provide users with IT facilities that are efficient and secure. However, there will always be the possibility that a security threat or vulnerability will exist. Scammers and hackers will always be there to take advantage of these weaknesses. The college cannot accept responsibility for any personal losses incurred by any individual through the use of its systems. Below is a brief summary of tips on how to remain safe when using a PC and being online;

9.1 It is important to bear in mind that web browsing is not a confidential means of communication and that the majority of web traffic is unencrypted and transmitted in a manner that can be intercepted by third parties (legally or otherwise).

9.2 Ensure that when you are viewing or entering sensitive data on a web browser, the browser must have an encrypted connection, at a very minimum. When this happens, you need to be aware that the web browser address bar should have a prefix of ‘https’ instead of just the usual ‘http’ (the ‘s’ stands for ‘secure’).

9.3 Users need to be aware of online scams such as ‘phishing’. This commonly involves a spam email and is designed by fraudsters to lure victims into divulging passwords, account details and personal and financial information. You will receive an email which will often ask you to ‘verify’ ‘validate’ ‘update’ or ’confirm’ your details, and may direct you to a bogus website. Any suspicious email should always be ignored and deleted. If unsure, contact the IT Service Desk for assistance.

9.4 Advertisement scams and rootkits (hidden viruses). Users should be very wary of clicking on 3rd party advertisements on websites (even on legitimate websites). This is because this space can be manipulated by malicious scammers. Clicking on such links can lead to you running a rootkits on your PC, often without the users’ knowledge.

9.5 Do not download any software direct from the Internet without consulting the IT Service Desk first. Downloading and installing un-trusted software could lead to the propagation of malware.

9.6 No reputable organisation will send out emails asking you to enter, confirm or validate personal/account details. If you are ever unsure about the authenticity of an email, try to verify the request by contacting the organisation through a different method of communication, such as the telephone.

9.7 IT keep backups of data stored on the central servers (H: L: & S: drives). It is advisable that all college data should be stored in these locations and any data stored on local machines will be the responsibility of the individual user to keep backed up. IT cannot be held responsible for the loss of any data stored on a local machine through either re-imaging of machines or failure of hardware.

The above sections briefly cover some of the basics with regards to inline security. For further detailed advice, users are advised to lookup the websites http://www.getsafeonline.co.uk and http://banksafeonline.org.uk. Other reliable sources of information are direct.gov.uk, ncsc.gov.uk, ico.org.uk and bbc.co.uk.

Should you need any further assistance or advice, please contact the IT Service Desk on 7016 or email ITServiceDesk@kirkleescollege.ac.uk