Lakes College West Cumbria

Quality Assurance

Policy: **Security Policy – Electronic Information Systems**

Policy Ref: **AP/7CA/SP103**

Approved By: **Karen Wilson**

Responsible Person: Andrew Sands

Date last reviewed: **09 January 2025**

Date of Next Review: **09 January 2026**

Approval Date: **03 December 2026**

Controlled Document

1. Statement of Intent and Scope

1.1. The policy covers:

- the deployment and use of the College's electronic information systems (i.e. all computers, peripheral equipment, software and data) within and between Lakes College - West Cumbria property, or belonging to the college but located elsewhere.
- the use of information systems not owned by the college and located outside of its property, where such use is affected from or via equipment located on college property, or by equipment belonging to the college.
- all use of the college's data and or communication network
- the security of hardware, software and data; the security of personnel using information systems; and the security of the college's assets that may be placed at risk by misuse of information systems.

1.2. In respect of copyright and data protection aspects, the policy covers the use of information systems not owned by the college or located on its property, but used by college learners, staff or representatives for study or business purposes connected with the college.

2. Objectives

2.1. Lakes College seeks to protect its assets from loss and to provide a secure working environment for its learners and staff. This needs to be balanced against the desire to make the full use of the potential of technology for working and learning as defined in the Teaching, Learning & Assessment Strategy. The objectives of this policy are to ensure as far as is reasonably possible that:

- the college's assets are secure against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence, and

- the college is protected from damage or liability resulting from use of its facilities for purposes contrary to the law of the land or against the rules and regulations sanctioned by the college's governing body.

Controlled Document

3. Legislation and Other Policy

3.1. The policy is to be read in the context of the following legislation:

- Data Protection Act 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Freedom of Information Act 2000

and any other relevant legislation.

3.2. The college has adopted as policy the Guidance (Appendix 3) issued by the Universities and Colleges Information Systems Association on the Computer Misuse Act.

3.3. The college is obliged to comply with, and endorses, the following:

- JANET Acceptable Use Policy, (Appendix 4), issued by the United Kingdom Education and Research Networking Association
- Code of Conduct on the Use of Software and Datasets, issued by the Joint Information Systems Committee of the Department for Education

4. Application of the Policy

4.1 Enforcement

It is the specific responsibility of the Digital Services Manager to ensure that the policy is carried out.

4.2 Individual Responsibility

All learners and staff have a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policy.

4.3 Breach

It is the duty of the Digital Services Manager to take appropriate action to prevent breaches of the policy. Where such action is outside of this remit, the Digital Services Manager will notify the appropriate Director or Business Support Manager.

4.4 Review and Audit

The Digital Services Manager is responsible for regular review of the policy ensuring that the policy is appropriate for the protection of the College's interests.

Controlled Document

5. Acceptable Use

Acceptable use is defined as use for the purposes of:

- Teaching and learning
- Research
- Personal educational development
- Administration and management of college's business
- Development work and communication associated with the above
- Consultancy work contracted to the college
- Reasonable personal use of computer facilities, where not connected with any commercial activity, is at present regarded as acceptable where this use does not interfere with work or study commitments.

5.1 The Acceptable Use Policy (Appendix 1), which forms part of the college's rules, are binding on all learners and will form part of the contract of employment for staff. The rules will be regularly reviewed by the Strategic Team for adequacy.

5.2 It is college policy that there will be guidelines set out in a Code of Good Conduct (Appendix 2) which will be reviewed regularly by the Strategic Team and circulated to all members of the college. Users are expected to abide by this code.

5.3 It is college policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

5.4 The Digital Services Manager has responsibility to take all reasonable steps to stop unacceptable use of information systems. This responsibility will be discharged through the Digital Services department, which will be guided on policy issues by the Strategic Team and appropriate external bodies.

6. Registration

6.1 The following are eligible to register as users:

- any learner on a course leading to a recognised qualification taught within and awarded by the college, or other full-time learner of the College;
- any person holding a contract of employment with the College;
- any person recommended by college managers for the approval of the Digital Services Manager.

6.2 With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users. The Digital Services Manager or relevant manager, as appropriate, has responsibility for implementing such access restrictions.

6.3 Please refer to the Access to College Accounts Procedure for more details.

Controlled Document

7. Advice and Training

7.1 It is the responsibility of the Digital Services Manager to ensure that all users are made aware of the risks of security breaches and of their responsibility to take adequate precautions.

7.2 It is college policy that good practice relating to security should be a concern of all IT training.

7.3 Documentation and publicity of IT facilities shall contain relevant advice on good practice relevant to security.

8. Destruction of Data

The following is in addition to the information found within the Data Protection Policy and outlines the procedures for the secure and compliant destruction of data held by Lakes College to prevent unauthorized access, loss, or misuse of sensitive and personal information. This is to ensure compliance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR) regarding the retention, deletion, and disposal of personal data. This applies to all employees, contractors, vendors, and third parties who manage or handle data on behalf of Lakes College. It covers both physical and electronic data destruction.

8.1 Data Retention and Deletion:

- Retention Period: Data should only be retained for as long as necessary to fulfill the purpose for which it was collected. Once data is no longer required, it must be securely destroyed.
- Data Review: Regular reviews of data storage must be conducted to ensure that outdated or unnecessary data is identified and appropriately destroyed.
- Destruction of Data: Upon reaching the end of its retention period or when it is no longer needed for operational purposes, data must be destroyed in compliance with the procedures outlined in this policy.

8.2 Destruction of Physical Data (Paper Records):

- Shredding: All paper records containing personal data or sensitive information must be shredded using a cross-cut shredder or another secure method that ensures the data cannot be reconstructed or accessed.
- Shredded material must be disposed of in a secure waste container. A third party waste disposal service is used to ensure proper destruction.

8.3 Destruction of Electronic Data:

- Data Deletion: Electronic data stored on computers, servers, or other digital devices must be deleted in a manner that prevents recovery.
- Hard Drive Destruction: Physical destruction of storage devices such as hard drives, USB drives, or other media is carried out by a certified professional destruction service.
- Cloud Storage: Data stored in cloud systems is deleted in accordance with the cloud provider's security protocols to ensure complete destruction.

8.4 Employee Responsibilities:

Controlled Document

- Employees must ensure that both physical and digital data they handle is securely destroyed when no longer required and report any incidents involving unauthorized access or mishandling of data to the Data Protection Officer (DPO) or relevant authority.
- All employees will receive regular training on data protection and secure data destruction practices.

9. Password Standards

The following are requirements and guidance for creating secure passwords using a three-random-words method to enhance security while maintaining simplicity and memorability.

- Passwords must be at least 12 characters long.
- Passwords must consist of three random words combined in a way that does not create a predictable phrase or common saying.
- Words can be separated by spaces, special characters (e.g., -, _, or #), or joined directly.
- Avoid using personal information such as your name, username, birthdate, or any easily guessable details.
- Avoid reusing passwords from other accounts or services.
- Passwords can include both uppercase and lowercase letters (A-Z, a-z).
- Passwords can include both numbers (0-9) and special characters (e.g., !, @, #, etc.) if desired.
- Users should use a password manager to store and manage passwords securely.
- Users should not share any personal passwords with others.

10. Remote Access Control

The following are guidelines to ensure secure remote access to Lakes College IT systems and data, ensuring the protection of sensitive information and minimizing security risks associated with remote work or external access. This applies to all employees, contractors, third-party vendors, and other individuals authorized to access Lakes College's IT systems remotely.

10.1 Authorized Users:

- Remote access to IT systems is only permitted for authorized personnel who require access to perform their job duties.
- Users must authenticate using strong, multi-factor authentication (MFA) methods.
- Remote access will be revoked immediately upon termination of employment or contract, or when access is no longer required for the user's role. For any support vendors, this termination is after the end of each session but can be recreated for the next piece of work.
- Users must report any lost or stolen devices used for remote access immediately to the Digital Services department.

Controlled Document

10.2 Secure Connections:

- All remote access must be conducted via approved secure connections.
- Unauthorized methods of access, such as direct connections without encryption, are strictly prohibited.

10.3 Device Security:

- Devices used for remote access must be secured with up-to-date antivirus software, encryption, and a secure lock screen. This ensures that devices are adhering to the Lakes College Cyber Essentials Plus certification.
- Personal devices used for remote access must be authorised by Digital Services and comply with Lakes College's minimum IT Cyber Security requirements. If they do not, access will be denied.

10.4 Access Restrictions:

- Users will have access only to the systems and data necessary for their roles. This ensures that a 'need to know' and 'zero trust' approach is used.
- All remote access sessions should be logged, monitored, and reviewed for unusual or unauthorized activity.

11. Remote Working

These guidelines are for the purpose of secure and compliant remote working, specifically regarding the use of IT systems, devices, and data access.

11.1 Remote Work Setup:

- Employees must use only company-issued or approved devices for remote working, which meet Lakes College's security standards. Personal devices (BYOD) must be registered with IT and secured according to the same standards.

- Remote workers must connect to Lakes College's systems via secure, encrypted connections (e.g., VPN, two-factor authentication). Public or untrusted Wi-Fi networks should be avoided unless a VPN is in use.

11.2 Data Access and Security:

- All devices used for remote working must be encrypted to protect Lakes College nata, particularly when accessing sensitive or personal data.

- All remote access to systems must be secured with multi-factor authentication (MFA) to reduce the risk of unauthorized access.

- Employees will have access only to the systems and data necessary for performing their job roles. Access privileges should be reviewed regularly to ensure they remain appropriate.

11.3 Data Protection Compliance:

- All employees working remotely must adhere to the requirements of the General Data Protection Regulation (GDPR), particularly regarding the secure handling and processing of

Controlled Document

personal data. Data should only be accessed or processed in accordance with Lakes College data protection policies.

- Personal and sensitive data should not be stored on personal devices unless required for business operations. If this is necessary, encryption and strong access controls must be used.

11.4 Device Security:

- Employees must ensure that their devices have up-to-date antivirus software and anti-malware tools installed. IT will provide support for installation and updates.
- In the event of a lost or stolen device, remote wipe functionality must be enabled. Employees must report any incidents of loss or theft immediately to IT for appropriate action.
- All devices used for remote work must receive regular updates and patches to protect against vulnerabilities.

11.5 Home Office Environment:

- Employees are responsible for maintaining a secure and confidential work environment at home or in any other remote working location. This includes physical security measures such as locking devices when not in use, using privacy screens, and ensuring that personal data is not exposed to unauthorized individuals.
- Employees must follow the guidelines provided by the Health and Safety at Work Act 1974 to ensure that their remote working environment is safe. This includes ergonomic workstation setup and ensuring that the environment is free from hazards that could pose risks to physical or mental health.

11.6 Communication and Collaboration:

- Remote workers should use only Lakes College approved communication tools (e.g., email, video conferencing) to conduct work-related activities. Unauthorized tools, such as personal email accounts or file-sharing services, should not be used for work purposes.
- Any sharing of data with third parties must comply with Lakes College's data protection policies. Employees should avoid sending sensitive data via unsecured channels (e.g., unencrypted emails).

11.7 Incident Reporting:

- Employees must immediately report any suspected or actual security incidents, such as data breaches, unauthorized access attempts, or lost/stolen devices, to the IT department.
- Lakes College will follow its incident response plan to mitigate any risks from security breaches, including notifying the Information Commissioner's Office (ICO) where required by law (under GDPR).

11.8 Monitoring and Compliance:

Controlled Document

- Lakes College reserves the right to monitor remote access to its IT systems to ensure compliance with this policy. Monitoring will be conducted in accordance with applicable laws and will focus on ensuring security, performance, and legal compliance.

- Employees working remotely must comply with all other relevant Lakes College policies, including but not limited to those covering data protection, information security, acceptable use, and intellectual property.

11.9 Employee Responsibilities:

- Employees are expected to maintain a secure and productive remote working environment.

- Employees should ensure that their remote working devices are not shared with unauthorized individuals and must take steps to prevent data breaches.

- Employees must immediately inform their manager or IT if they experience technical issues that impact their ability to work securely.

11.10 Employer Responsibilities:

- The employer is responsible for providing employees with the necessary tools and support for secure remote working, including VPN access, secure communication tools, and device management solutions.

- IT will provide employees with regular cybersecurity training to ensure they understand the risks and best practices associated with remote working.

12. Mobile Computing

The following points define the security requirements for the use of mobile devices (e.g., smartphones, tablets, laptops) for accessing, storing, and transmitting Lakes College information. This aim is to protect Lakes College's data and systems from unauthorized access, loss, or misuse, and ensure compliance with relevant UK data protection and cybersecurity regulations, including GDPR and the Data Protection Act 2018 (DPA).

Only authorized mobile devices, including smartphones, tablets, and laptops, may be used for accessing Lakes College network and data.

12.1 Security Requirements:

Controlled Document

- Password Protection: Devices must be secured with strong passwords, pin codes or biometric authentication (e.g., fingerprint or face recognition). Passwords should adhere to Lakes College's password policy for strength and periodic changes.

- Multi Factor Authentication (or 2 Factor Authentication) must be setup for each device and application that are used. This must be via the approved MFA solutions in place at Lakes College.

- Mobile devices must have the latest security updates and patches installed as soon as they are available.

- Users are required to regularly update their mobile devices to ensure they are protected against known vulnerabilities.

- In the event of a lost or stolen mobile device, the user must immediately notify the Digital Services department to trigger remote wipe and disable access to corporate systems.

- Mobile devices should only connect to trusted networks and should avoid using public Wi-Fi for accessing sensitive or confidential data.

- Employees are encouraged to use company-approved mobile hotspots and secure remote connection service solutions when working remotely.

- Mobile devices issued by Lakes College will be locked down, with only approved apps permitted to be installed.

- Employees are responsible for ensuring that their mobile devices comply with this policy and must immediately report any security incidents, such as lost or stolen devices, unauthorized access, or data breaches.

- Employees must take reasonable precautions to protect their mobile devices from theft, damage, or unauthorized use (e.g., not leaving devices unattended in public places).

13. Operational Practice

13.1 It is the responsibility of the Digital Services Manager to attend to the following:

- securing the integrity of data and code held and processed on the college's information systems;
- securing the integrity of all computers;
- ensuring that there is no storage of inappropriate material on College systems;
- in the event of a suspected security breach, enforcing appropriate restrictions to the service until confidence is restored;
- provision of appropriate security tools for use by learners and staff on computers under their control;
- provision of effective controls on access to restricted facilities (e.g. administrative computers).

13.2 It is the responsibility of the computer user to attend to the following:

- taking appropriate security precautions in respect of computers under his/her control;

Controlled Document

- observing good practice recommendations for security in respect of facilities provided on multi-access computers and networks.

13.3 Damage to equipment, software or data resulting from failure to observe this policy is deemed to be the responsibility of the defaulter.

13.4 Control of access to personal data is the remit of the Deputy Principal, who will ensure that information about rights and responsibilities under the Data Protection Act (2018) is made available.

Controlled Document

14. Monitoring

The Digital Services Manager or the relevant manager, as appropriate, is responsible for ensuring that usage of resources will be logged in sufficient detail to identify defaulters where technically possible.

14.1 The Digital Services Manager will authorise Digital Services Staff whose duties require it to monitor and police the use of computer facilities. Monitoring data will be collected only to assist investigation of a suspected security breach or other misuse.

14.2 Digital Services support staff shall not monitor personal information except in specific instances where a suspected breach of security or other substantive offence requires it. Every such incident will be reported to the college Principal, where the suspected offender is a learner, or otherwise to the Head of Human Resources/Deputy Principal. Details of the incident will be logged.

14.3 The Digital Services Manager is empowered to authorise a software audit of college equipment, where it is deemed necessary.

15. Duties of Digital Services Staff

15.1 Digital Services Staff have responsibility for maintaining the integrity of computer systems and data held on them, and for ensuring the systems are not misused.

15.2 Digital Services Staff are provided with privileged access to computer systems in order to carry out their responsibilities. They have a duty to always use such privileges in a professional manner and within the interest of the college.

15.3 The Digital Services Manager is responsible for ensuring that the duties of Digital Services Staff are carried out.

15.4 The Digital Services Manager will publish and maintain details of Digital Services Staff and the domain of their responsibilities.

Controlled Document

- **Appendices**

Appendix 1 Acceptable Use Policy

Appendix 2 Code of Conduct
Appendix 3 Guidance on Computer Misuse Act
Appendix 4 JANET Acceptable Use Policy - links

- **References**

Learner Disciplinary
Disciplinary Procedure for Staff

Controlled Document

OVERVIEW

Policies

Overarching policy — Security Policy

This is the basic agreement with all users which they accept when logging on to the network — Acceptable Use Policy — Appendix 1

Guidance Notes

A clear set of guidelines to help users follow the policies above. — Code of Conduct — Appendix 2

Guidance on one of the main areas of law governing these policies — Guidance on the Computer Misuse Act — Appendix 3

Links to documents outlining our obligations with respect to the JANET link (our connection to the internet) — JANET AUP — Appendix 4

APPENDIX 1

Acceptable Use Policy

Contents

This document is the Acceptable Use Policy (the **"AUP"**) which must be followed and accepted by all users of the College's electronic information systems (the **"network"**). "**User**" refers to anyone who has access to the College network, whether they are an employee, learner or other person authorised to use the network.

The ability to use the College's network (including email and the internet) provides many opportunities for the College as it facilitates the gathering of information and communication with fellow employees, learners, customers and other contacts. However, this access opens up the College to new risks and liabilities. It is therefore essential that all users of the network read this Acceptable Use Policy, and make themselves aware of the potential liabilities involved in using the College's network.

The College has an overall Security Policy governing the management of electronic information systems.

In addition, the College has issued a Code of Conduct as guidelines of expected behaviour and good practice when using the College's network.

Controlled Document

- **Acceptable Use Policy**

1.1 The College has the right to monitor any and all aspects of its telephone and computer system that are made available to you and to monitor, intercept and / or record any communications made by users, including telephones, e-mail or Internet communications. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 users are hereby required to expressly consent to the College doing so. In addition the College wishes to make you aware that Close Circuit Television (CCTV) is in operation for the protection of employees and learners.

1.2 Permission needs to be sought from the Digital Services Manager or Deputy Principal to review network use history, including email/web history, if inappropriate use is suspected.

1.3 Electronic information systems administered by Lakes College West Cumbria may be used only by learners and staff of the College and other persons authorised in writing by the Digital Services Manager.

1.4 The information systems are used on the understanding that the College will not accept any liability whatsoever for loss, damage, or expense which may result from the computing facilities, except to the extent that such loss, damage, injury or expense are attributed to negligence or breach of statutory duty on the part of the College or any of its servants or agents acting in their capacity as such.

1.5 Access gained through permitted use of the College's computers to other computing centres and facilities linked to those at this College is governed by this Acceptable Use Policy, in addition to any rules in force for use of the facilities at the remote site.

1.6 Your 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. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

1.7 Usernames and other allocated resources shall be used only by the registered holder. Users shall maintain a secure password to control access to their usernames on multi-user systems. Sharing of usernames will not be permitted save in exceptional circumstances by prior agreement of the Digital Services Manager. You are responsible at all times for safeguarding your passwords for the system. For reasons of security your individual password should not be printed, stored on-line or given to others. User password rights given to users should not give rise to an expectation of privacy.

1.8 No person shall by any wilful or deliberate act or by failure to act with due and reasonable care jeopardise the integrity of the computing equipment, its operating systems, systems programs or other stored information, or the work of other users, whether within the College or in other computing locations to which the facilities at the College allow connection.

1.9 Unauthorised access to computer material (i.e. a program or data) and unauthorised modification of computer material are forbidden by law (Computer Misuse Act 1990) and by these Rules, which endorse the Guidance on the Computer Misuse Act (originally published by the Universities and Colleges Information Systems Association), copies of which may be obtained from Digital Services Department.

Controlled Document

1.10 Use shall not be made of facilities at other locations if a charge for such use will be incurred by the College unless such use has been authorised in writing by the Digital Services Manager. Any charges incurred in contravention of this rule will be reimbursed by the user.

1.11 Computer facilities available for use within the College may be used only for:

- Learning and teaching
- Research
- Personal educational development
- Administration and management of College business
- Development work and communication associated with the above
- Consultancy work contracted to the College

1.12 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 be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material as appropriate.

1.13 No person shall use, copy or transmit any software from College equipment unless a licence from the copyright holder is in force. Any restrictions placed on the use of equipment administered by the College must be observed.

1.14 College network users should not import non-text files or unknown messages on to the College's system without first having them scanned for viruses.

1.15 No person or persons shall use the College's information systems to hold or process personal data except in accordance with the provisions of the Data Protection Act 1998. Any person wishing to use the facilities to hold or process personal data shall be required to inform in advance the Digital Services Manager, to comply with any restrictions the College may impose concerning the manner in which the data may be held or the processing carried out.

1.16 All use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

1.17 Users should not access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. Users should not make derogatory remarks about employees, learners, competitors or any other person. Any written derogatory remark may constitute libel. You should be aware that such material may also be contained in jokes sent by e-mail. Such misuse of the network will be misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any user's e-mail in any disciplinary process.

1.18 Reasonable private use of the network is permitted but should not interfere with your work or study. The contents of personal e-mails, sites and services accessed must comply with the restrictions set out in these guidelines. Excessive private use of the network during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

1.19 By sending e-mails on the College's system, you are consenting to the processing of any personal data contained within that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the College to process such data you should communicate it by other means.

Controlled Document

1.20 Computer and e-mail accounts are the property of the College and are designed to assist in the performance of your work. You should, therefore, have no expectation to privacy in any e-mail sent or received, whether it is of business or personal nature.

1.21 College users must never engage in political discussions through outside newsgroups using the College's network.

Breaches of this Acceptable Use Policy are offences under the rules of the College and are addressable under these rules.

If after investigation it appears prima facie that a member of the College staff or a learner has acted in breach of these rules, he or she may be denied access to all computer facilities pending the conclusion of disciplinary proceedings against him or her.

Controlled Document

Appendix 2

Code of Conduct

Contents

Controlled Document

The College has a Security Policy governing the use of the College's electronic information systems (the **"network"**), and an Acceptable Use Policy (the **"AUP"**) which must be followed.

In addition, the College's Strategic Team has issued the following Code of Conduct as guidelines of expected behaviour and good practice when using the College's network.

1. What you may use the College's network for

Digital Services are provided primarily for academic purposes or for College business. There is no objection to your making reasonable use for personal purposes such as electronic mail or preparing CVs, providing you observe the following code:

- Don't waste materials, or waste time on the College network to the detriment of others.
- Don't send offensive, or unsolicited junk, or nuisance mail, attachments or messages. Also remember mail might reach somebody for whom it was not intended.
- Your use must be lawful, honest and decent, and must have regard to the rights and sensitivities of other people. This means that any use that is or could be considered obscene or with the intent of annoying or offending somebody else is forbidden.
- Don't use the College network for commercial gain.
- The law requires that you don't hold any information in electronic form about living persons unless you are registered to do so. (see Section 9)

- **Respect the equipment**

Please treat computer equipment with respect - it is there for your benefit.

- Please be considerate of other people - avoid excessive noise or other nuisance.
- No eating or drinking in whilst using computer equipment.
- Don't run your own software on College computers or load software on to the computer unless you have explicit permission to do so from the Digital Services Department.
- Don't delete, disable or tamper with any software provided by the College.
- Don't tamper with the hardware or any network or power connections.

- **Using the Network**

- **Never** attempt to gain access to another account (username or file store) unless you have been given explicit permission to do so by the Digital Services Manager. If you do you are breaking the law.
- Do not connect your own equipment to the network, with the exception of the LCWC-Guest wireless network which is provided for this use.

- **Emails and the Internet**

- E-mails should be drafted with care. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and the communication can be recovered even when it is deleted from your computer.
- Try not to create e-mail congestion by sending trivial messages or unnecessarily copying e-mails. Employees should regularly delete unnecessary e-mails to prevent over-burdening the system.
- Make hard copies of e-mails which you wish to keep for record purposes.
- You may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone to confirm receipt of important messages.

Controlled Document

- **Look After Your Usernames and Passwords**

All learners and staff are entitled to use the computer network service. Once learners have enrolled they will receive a username and password as part of their induction; staff will receive this as part of their staff induction.

- It's **your** responsibility to keep your logon details secure. **Never** allow anyone else access to it.
- **Keep your password secret**; don't use your name, your partner's name, your car registration or anything else that someone might guess. If you have to write it down, disguise it. Change your password regularly. If you think someone might have watched you typing it in, change it immediately.
- Don't leave a logged-in session unattended, even for a moment.
- Make sure you **log out** when you finish using the computer.
- **Never** use anyone else's account, with or without their permission.

- **Look After Your Equipment**

It's **your** responsibility to keep equipment under your control free from viruses or anything else with the potential of causing damage. The College uses virus protection software centrally and on all its computers.

- **Look After Your Data**

You, not the College, are ultimately responsible for the security of your data. If you hold important data on a multi-access computer, you should not rely entirely on the College's back-up procedures. Wherever possible, keep an independent copy of your data.

Power, disk and system failures usually take effect without warning; consider the consequences before you use the computers. The following good practice is recommended:

- Save your files at frequent intervals.
- Keep your own multiple back-up copies of anything that is important.
- Read the messages displayed at log-in on the Intranet; this facility is intended to warn you of any imminent service interruptions.

It is sometimes possible to retrieve files that have been deleted accidentally, but you shouldn't rely on this feature. When you leave the College your account and files will be deleted. Any usernames provided for use on a particular course will be deleted at the end of the course. It is your responsibility to take a copy of anything you need before you finish.

- **Observe Copyright Restrictions**

Don't copy any software without permission. You should assume software is copyright unless you know otherwise.

Don't copy any data without permission. This includes copying text or graphics - whether by using a scanner or by typing it in. The usual exceptions to copyright arrangements which allow you to photocopy parts of an article or book **do not apply** to the use of computers.

Controlled Document

- **Respect Personal Information**

The college has a Data Protection Policy with which you should be familiar.

You are obliged by law to keep any personal data secure, whether it is your own or someone else's. This means you should not share personal data with anyone who doesn't need it, or send it by email without encrypting the information first. Do not store personal data outside of the college network.

As an example, do not take or transfer images of learners or staff without the express permission of the subject (or parents/carers as appropriate).

- **Rules and Discipline**

You are bound by the college's Security Policy and Acceptable Use Policy. You will have received a copy when you joined the College and are reminded of them at each login to the College's network. You should ensure you are familiar with these rules. You can obtain another copy from the Learning Resource Centre, the College's website or the Digital Services Department.

If you break the Rules:

- Your permission to use College computers may be withdrawn.
- You are also liable to disciplinary action under College procedures.

If you believe you have been treated unfairly you have the right of appeal to the College Principal (if a learner) or the Head of Human Resources (if not a learner).

Controlled Document

APPENDIX 3

Guidance on the Computer Misuse Act

Contents

1. Introduction

The Computer Misuse Act became law in August 1990. Under the Act hacking and the introduction of viruses are criminal offences. Lakes College needs to co-operate to take action under the Act as the offences may potentially be committed by members of the college, students in particular, and are often perpetrated on machines or networks within the college. For offences committed the College may wish to use the speedier process of internal disciplinary measures (attached) rather than resort to the law. The aim of this Guidance is to ensure that colleges recognise the seriousness of these offences and to encourage a greater degree of common practice in dealing with the people who carry out these actions, whether action is taken under the criminal law or through the use of disciplinary procedures.

The following sections describe the types of offence and suggest a range of internal penalties.

2. Definition

The Act identifies three specific offences:

- Unauthorised access to computer material (that is, a program or data).
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
- Unauthorised modification of computer material.

The Act defines (1) (the basic offence) as a summary offence punishable on conviction with a maximum prison sentence of six months or a maximum fine of £2000 or both. The Act goes on to describe offences (2) and (3) as triable either summarily or on indictment, and punishable with imprisonment for a term not exceeding five years or a fine or both. These sentences clearly reflect the perceived gravity of the offence and would imply that colleges should take an equally serious view of hacking or virus proliferation.

Controlled Document

Universities and Colleges are primarily concerned with preserving the integrity of shared academic computer systems and of all administrative systems. In the event of any problem the Digital Services Manager would expect to take immediate remedial and preventive action and would expect the institution to back them up in this action with penalties in place which would serve to discourage hacking, particularly the third category which could result in a student's work being destroyed or in a complete system failure.

Definitions of Unauthorised Access in the Higher Education Context

The offences described in the Act can be interpreted within the university and college scene and perhaps extend into areas which in the wider context would not be considered to be offences. The examples given below are intended as a guide to the seriousness of the offence and do not attempt to cover all eventualities.

Example 1: Unauthorised Access to Computer Material

This would include: using another person's identifier (ID or username) and password without proper authority in order to use data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data (for example, to a screen or printer); laying a trap to obtain a password; reading examination papers or examination results.

The response to some actions will depend on the specific conditions of use in force. Take, for example, unauthorised borrowing of an identifier from another student in order to obtain more time for a computer project the student was required to complete. In this case both the student who borrowed the ID and the student who lent it would be deemed to have committed an offence.

Example 2: Unauthorised Access to a Computer with intent.

This would include: gaining access to financial or administrative records, but intent would have to be proved.

Example 3: Unauthorised Modification of Computer Material.

This would include: destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a complete system malfunction.

Universities and Colleges should recognise that action under disciplinary procedures is more effective if a similar view is taken across the sector and if institutions are prepared to discipline their students for offences carried out across the network on the facilities of other universities and colleges. It is desirable that as far as possible similar offences in different institutions carry similar penalties.

Controlled Document

3. Action to Deal with Misuse

Preventive Measures

The simplest form of preventive action is publicity, and all opportunities should be used to make it clear that the universities and colleges do not tolerate this type of behaviour. The conditions of use for computing facilities should spell out the seriousness of these activities.

Preliminary Action

The status of the senior managers responsible for information systems can vary from one institution to another. It is assumed that in every university such senior managers have the authority to suspend access to the facilities for which they are responsible. The institution should support such action and ensure that managers with responsibility for local systems have the knowledge and the authority to take similar action. Such suspension of access would be a likely initial response to any misuse.

Computer Security

The then Computer Board circulated to universities in March 1989 advice on measures to combat hackers. With the Computer Misuse Act coming into force these measures assume even more importance.

Identifying the Offender

Finding and identifying someone who has hacked into or misused a system is a difficult and, above all, time consuming task. It is sometimes possible to identify the person uniquely. More often it relies on producing sufficient circumstantial evidence to persuade the offender to admit that he perpetrated the offence.

4. Penalties under the Disciplinary Procedures

Care needs to be taken when assessing the level of punishment. University and college disciplinary procedures may not need the strict proof required by criminal law and thus may need to consider only the balance of probabilities. However, institutions should ensure that the standard disciplinary procedures do satisfy the requirements of natural justice. A narrow line needs to be taken between making the penalties so severe that they are never implemented and being so lax that hacking and other misuse is treated as just a game.

The least serious offences could be punished solely by temporary withdrawal of the facilities together with a formal warning from an appropriate person, such as tutor or head of department for a student or line manager for a member of staff. However, such a warning must be recorded, as a second offence clearly becomes much more serious.

The next point on the scale could be a fine, for those universities which use such systems, or a fixed period, set at an appropriate level, of withdrawal of access to computing resources. For the more serious offences of category (2) and category (3) the minimum penalty should be withdrawal of all computing resources for a term but the normal penalty should clearly be more severe and commensurate with the degree of intent and seriousness of the offence. The consequential effects of withdrawal of facilities should be borne in mind, including the fact that consequential effects will vary in each case. For example, withdrawal could have the effect of forcing a student to repeat examinations or to repeat a year. If the person has already been warned, or if the disruption is intentional or severe, then more severe penalties should be invoked. For a student it is suggested that they should not be allowed to continue the course.

Controlled Document

5. Initiating Legal Procedures

Universities and colleges should be prepared to use the full powers of the Act for serious offences whether they originate within or without the higher education sector. It is normally the responsibility of the Police to initiate any action, but for a prosecution to be successful, evidence needs to be collected and kept as soon as misuse is suspected. Universities could well need to seek technical and legal advice early in the proceedings.

6. Summary

- The definitions of computer misuse in the Act should be used.
- A range of penalties, matched to the offence, should be recognised, from suspension of use of computer facilities for varying lengths of time, through fines to the ultimate sanction of being sent down; legal sanctions should be invoked where appropriate.
- Second and subsequent offences should be treated increasingly more severely than first offences.
- Offences committed on other the facilities of other institutions should be treated at least as severely as offences committed on local machines.

7. References:

Computer Misuse Act 1990, Chapter 18, ISBN 0-10-5418900.
Computer Board paper: Specific Measures to Combat Hacking, March 1989.
Learner Disciplinary
Disciplinary Procedure for Staff

Controlled Document

APPENDIX 4

JANET Acceptable Use Policy

The latest version of the JANET Acceptable Use Policy can be found here:

https://community.jisc.ac.uk/library/acceptable-use-policy

JANET(UK) Contact Details and URLs

JANET Terms:
https://community.jisc.ac.uk/library/janet-policies/terms-provision-janet-service

JANET Policies:
https://community.jisc.ac.uk/library/janet-policies

JANET Service Desk: service@ja.net, 0870 850 2212

JANET CSIRT: irt@csirt.ja.net, 0870 850 2340

Controlled Document

12 Initial Screening for Equality Impact Assessment (including Safeguarding)

To be completed prior to a Policy or Procedure being introduced and at each review.

Name of Policy/Procedure:	
Is this a new or existing policy/procedure? □ New □ Existing	
1. To ensure that the policy / procedure complies with the Equality Act 2010, which of the listed categories could be impacted by the policy / procedure? (The categories follow the College Single Equality Policy, and the impact could be positive or negative.) □ Age □ Compliance with Children & Families Act 2014 □ Disability □ Gender □ Race/ethnicity □ Gender Re-Assignment □ Marriage/Civil Partnership □ Pregnancy/Maternity □ Socio-Economic □ Sexual Orientation □ Religion/Belief □ All of the above □ None of the above expected	
2. What are the risks of introducing this policy / procedure change to any of the above groups?	
3. What are the expected benefits of introducing this policy / change to any of the above groups?	
4. Are there any areas or issues that could impact on the safety of staff or learners?	
5. What evidence do you have for your responses to questions 2, 3 and 4? (e.g. evidence could be provided to counteract identified risks and, therefore, a full screening would not be required)	
6. What is the level of risk for the policy / procedure?	□ High □ Medium □ Low
7. Is a Full Screening Impact Assessment required?	□ Yes (complete the box below) □No
What are the recommendations from Equality Impact Assessment?	

Controlled Document

Date of Review:	
Reviewer's Name:	
Reviewer's Job title:	

Controlled Document