

**IT POLICY, PROCEDURES AND GUIDANCE**

**Contents**

1. Summary

2. Introduction

3. Service and Support

4. Security

5. Software

6. Procurement of IT Equipment

7. The College Network

8. Access to the College Network

9. E-Safety

10. Management of the College Website

11. Remote and Wireless Access

12. Mobile Devices

Appendices

A ICT Systems Changes

B Protection and release of Staff or Student personal data

C Computer Passwords

D Computer Systems Generic User Accounts

E Computer Systems User Logon Accounts for Students/Staff who have left the College

F Creation of Staff & Non-Staff Network User Id

G Student Computer Use

H E-Safety for Staff – keeping safe whilst using computer systems

I E-Safety for Students – keeping safe whilst using computer systems

J Remote & Wireless Access to College ICT Systems and Data

K College Information Systems Support & Maintenance

L Protection of College Information & Communication Technologies

M Security backup of College data

**1. Summary**

This policy and guidance document is presented as a core document (overview) followed by a series of 13 appendices where the details under various headings can be found. The table of contents produces a quick summary to the appropriate sections of the document.

**2. Introduction**

The purpose of this document is to embed the Computer Services: Detailed Strategy 2016-20 and inform College staff and students of what can be expected in terms of Information Technology (IT). This covers the use of all computers and other related hardware such as printers and projectors and the use of the network infrastructure. In the following, the use of computers connected to the College network both for academic and administrative purposes is covered together with the procurement of IT equipment and the maintenance and support of it by the College.

**3. Service and Support**

**3.1 Structure**

At the heart of the College's IT structure is the Computer Services Department. The ICT Manager is responsible for the day-to-day running of IT services and is responsible to SMT for all aspects of the College's IT service, support and development. In addition there is a Marketing Manager who is separately responsible for the development of the College's website and for web communications.

**3.2 Support Priorities in order of priority**

* To ensure the IT infrastructure remains in operation, including both network and servers. From time to time upgrades and developments to the network and servers will be necessary and will take high priority in order to minimise overall disruption and to accommodate on-site contractors.
* Mission Critical services, including EBS, Payroll, Dream Accounts, Shared Printers and Telecoms.
* Curriculum priorities, including the College VLE.
* The College computer rooms, ensuring these remain fully operational.
* For the single-user, including breakdown of an individual computer or other college owned peripheral devices, and software problems.
* Current students with critical problems involving their own personal hardware or software problems.
* Help and advice on equipment, software upgrades and general IT requests from Support and Curriculum staff.

Notwithstanding the above ordering it will be open to either the ICT Manager to escalate a support request if it has consequences for the operation of an immediate College activity. Also, in the event of a Critical Incident the College Critical Incident Plan will take priority.

**4. Security**

**4.1 Network and Computers**

Security of the College’s network and of the computers used for the administration of College business is a crucial aspect of the IT policy. For this reason, only Computer Services staff or personnel working with Computer Service Staff will make changes to IT hardware or infrastructure and no server-specific hardware will be introduced to any College systems without prior consultation with the ICT Manager. See Appendix A for details.

**4.2 Firewall**

The College network incorporates a Juniper firewall, incorporating Smoothwall web filtering, to control data traffic into and out of the local network. This increases the security of the network and helps to keep the threat of malicious attacks to a minimum and to keep confidential information secure.

**4.3 Anti-Virus, Anti-Spam**

The College employs Windows 10 anti-virus and Barracuda Anti-Spam solutions to back up the firewall.

**4.4 Retention of Data**

Further background information is provided in Appendix B.

**5. Software**

The College takes seriously breaches of software licence agreements and piracy with respect to software packages. Only Computer Services staff will deploy changes to software. No software will be introduced to any College computer systems without prior consultation with the ICT Manager. See Appendix A for details.

**6. Procurement of IT Equipment**

IT equipment used by the various College Departments is procured by the ICT Manager – usually as part of the College’s Capital Resource Bid procedure.

In ordering equipment for the College, the Computer Services Operations Manager will ensure that full use is made of educational and other discounts and will ensure that an up-to-date inventory exists for all such equipment, including mobile devices. This is to ensure timely upgrades of equipment and to assist in cases of theft leading to insurance claims.

**7. The College Network**

The College network comprises optical, wired and wireless connections throughout the various college sites. Switches and wireless access points are the property of the College and are maintained by the College for its academic pursuits and its administration. Only contractors engaged by the Computer Services Department and the members of the Computer Services Department shall have direct access to any hardware component of the network, and interfering with any part of the wiring, optical fibres and hardware by any other college member will be deemed to be a serious matter.

**8. Access to the College Network**

All staff, students and visitors who use the College computer system must be issued with a valid and current user ID, which can be obtained from the Hex or Computer Services Helpdesk.

For details see Appendices C - G

Users are not permitted to use College IT or network facilities for any of the following:

* Any unlawful activity;
* The creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material;
* The creation, transmission, or display of material which is designed or likely to harass another person;
* The creation or transmission of defamatory material about any individual or organisation;
* The sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;
* The sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;
* The transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;
* The creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;
* Private profit, except to the extent authorised under the user's conditions of employment or other agreement with the College; or commercial purposes (including advertising commercial services) without specific authorisation;
* Gaining or attempting to gain unauthorised access to any facility or service within or outside the College, or making any attempt to disrupt or impair such a service;
* The deliberate or reckless undertaking of activities such as may result in any of the following:
  + The waste of staff effort or network resources, including time on any system accessible via the College network;
  + The corruption or disruption of other users' data;
  + The unauthorised access, transmission or negligent loss of data;
  + The violation of the privacy of other users;
  + The disruption of the work of other users;
  + The introduction or transmission of a virus or other malicious software into the network;
* Activities not directly connected with employment, study, or research in the College (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.

Please be aware that computers on a high bandwidth network such as ours are a prime target and new vulnerabilities are discovered every day. You are encouraged to take great care when opening email attachments. The Computer Services team will advise you on sensible precautions as necessary.

**9. E-Safety**

Staff

For the steps that should be taken to help keep staff safe whilst using the internet see Appendix H.

Students

For the steps that should be taken to help keep students safe whilst using the internet see Appendix I.

**10. Management of the College Website**

The College's website is managed by the Marketing Department and is maintained off-site.

**11. Remote and Wireless Access**

With the ever increasing use of mobile equipment used to access the College network remotely or via Wi-Fi, it is necessary to define standards for such access. These standards are designed to minimise the potential exposure to the College from damages which may result from unauthorised use of College resources.

Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical College internal systems, etc.

For details of the standards see Appendix J.

**12. Mobile Devices**

Mobile devices are becoming increasingly common and sophisticated. These range from tablet computers and iPads to smartphones. The College only supports the acquisition and maintenance of mobile phones (including smartphones) and other mobile devices where a person's work requires the use of such devices. In these cases the choice of network (carrier) will be at the College's discretion using a corporate account. Use of such College-owned devices should be related only to calls and emails made in the context of College activities.

**13. Business mobile phone policy**

Mobile phones may be provided to staff that would benefit from having a business phone available to them to make / receive business calls whilst away from the office. The allocation of a phone will be by agreement with the budget holder and would be given on a permanent basis for regular use in connection with their work.

Computer Services manages the mobile phone contract and all matters regarding the use of mobile phones should be referred to the Computer Services Department in the first instance. If you are issued with a mobile phone you are responsible for its security whilst it is allocated to you. It remains the property of Lancaster & Morecambe College at all times and shall be returned to Computer Services when you leave the employment of the College or it is no longer required as part of your job, or if the College requests its return for whatever reason.

In accordance with legislation, you may not use hand held mobile phones or similar device(s) whilst operating machinery, driving or any other activity which may put you or others at risk of harm.

**PROCEDURE FOR THE ALLOCATION OF MOBILE PHONES**

If your work is such that you would benefit from having use of a mobile phone, you will require your Line Manager and Head of Department’s approval. If you are regularly out of the office either on campus or off campus on official College business then it is likely that a phone will be specifically allocated to you.

All requests for mobile telephones must be completed on a ‘Request for a Mobile Phone’ form *(see ‘Forms’ section of the Hub)* and authorised by the Budget Holder. A full rationale must be provided with the request. Reasons for the request could be for one or more of the following reasons:

* Health and safety / security reasons especially for staff who are engaged in a substantial amount of travelling on behalf of the College;
* Staff engaged in business during unsocial hours i.e. before 7.00 a.m., after 7.30 p.m. and weekends;

* Staff who could be called upon to provide attendance at the College at short notice, such as those named officers listed in the College’s Emergency / Business Continuity Plan;
* Staff who are required to work outside of a teaching / office / workshop environment as part of their routine duties and responsibilities and have only intermittent access to landlines;
* The Budget Holder’s view is that a mobile phone is necessary for the role.

Following approval, the mobile device will be ordered by Computer Services and issued directly to the member of staff, the cost of the phone usage will be recharged to the relevant budget holder.

Where the need for a mobile phone is likely to be sporadic, you may borrow a phone from Lancaster & Morecambe College Reception for the duration of your need (ad hoc use). This may be, for example, to attend a meeting off site or if you are working from home during which time you must be contactable for business purposes. You must advise your manager when you have borrowed a College mobile phone and the phone number you will be available on.

If you leave the employment of Lancaster & Morecambe College or you no longer wish to have a phone allocated to you, you must return the mobile phone to Computer Services. Any outstanding personal call charges may be deducted from your final salary payment or, subject to timescales, a bill issued to you for repayment within 28 days.

**PERSONAL CALLS (P)**

This mobile phone policy acknowledges that mobile phones will only be issued to those staff who have a business need, whilst a small supply of unallocated phones are available for those who have an occasional business need. Because no member of staff holds a mobile phone that is not essential for business, no tax liability arises.

Staff should not use college mobile phones for personal phone calls.

The only exceptions are:

* a safe arrival call to home following travel to somewhere that involves staying away overnight;

* a brief call to let family know of any travel delays;
* a brief call to confirm travel arrangements, for example, to ask to be collected from the station;
* a brief call to make arrangements at home, for example, care arrangements when these could not be made in advance;
* calls home when staying overnight;
* in case of an emergency situation where it would be deemed reasonable to use the phone.

**COURTEOUS USE OF MOBILE PHONES**

Mobile phones should be switched off during meetings, lectures, seminars, training courses etc. except in very exceptional circumstances where it is vital to make or receive an urgent business call. In such circumstances you should adjust the phone to ‘silent’ mode and alert colleagues to the fact an urgent call needs to be made or is expected.

You should take due care of the phone at all times so that it is kept in good working condition. Any damage or theft / loss of the phone should be reported immediately to Computer Services. The phone must be PIN code protected and kept locked at all times to minimise security risks, particularly if the phone is stolen.

**APPENDIX A**

**ICT SYSTEMS CHANGE**

1. **Software Change and Deployment**

* Only Computer Services staff will deploy changes to software.
* No software will be introduced to any College computer systems without prior consultation with the ICT Manager.
* Computer Services Staff will raise a System Change Form which will describe the work to be undertaken.
* A target date will be set and personnel will be assigned to the job after consultation with the manager responsible for the ‘customer section’ and the release notes (if available) have been considered.
* An impact analysis and risk assessment will be completed and agreed by the ICT Manager.
* All changes/additions may be done on the Computer Services test bench following full testing procedure and documentation will be completed for all tests. Changes to user-facing and key systems will where possible be made out-of-hours. System downtime will be also be out of normal working hours where possible.
* Software changes/additions will be made to the live system primarily in the College holidays.
* Updates and patches that are extremely critical may be installed and implemented at times agreed with the ICT Manager and the Senior Management Team.
* All Computer Services staff will be made aware prior to any changes to the live system.
* All changes will be fully documented.
* The Computer Services Team will be made aware of any changes and their likely effects at the team meeting prior to the changes.
* Each system change will be completed independently. Only one change will be done and tested at any one time.

**2. Hardware and Infrastructure Changes**

* Only Computer Services staff or personnel working with Computer Service Staff will make changes to ICT hardware or infrastructure.
* No server-specific hardware will be introduced to any College systems without prior consultation with the ICT Manager.
* Computer Services Staff will raise a System Change Form which will describe the work to be undertaken.
* Following consultation with the customer a target date will be set and personnel will be assigned to the job.
* An impact analysis and risk assessment will be completed.
* All Hardware changes/additions will be tested and documentation will be completed for all tests.
* Hardware changes/additions will be made to the live system primarily in the College holidays. Changes requiring any down-time will be made out-of-hours where possible, or where this is not possible at a time to minimise any impact.
* In emergency situations, system resets/reboots will, whenever possible, be undertaken with agreement between the ICT Manager and SMT.
* All Network Officers will be informed prior to any changes being made to the live system.
* The Computer Services Team will be made aware of any changes and their likely effects at the team meeting prior to the changes.
* All logs will be updated.

**3. Security Software/Virus Checking**

* Virus updates are managed automatically by the Anti-Virus Application and the Network Security Officer receives e-mail notification of the latest threats.
* The Anti-virus system is updated automatically on all server and client systems.
* Virus alerts are sent to the Security Officer for remedial action.
* All changes are documented in the same way as other software updates.
* All logs are updated

**4. Password Changes/Data Movement/Storage Management/Access Management**

* Any changes in these categories will be done by the person manning the Customer Service Desk (or their nominee).
* Password resets can be requested verbally, but users must produce proof of identity prior to their password being changed.
* Student data will be moved on receipt of email confirmation from the student or a member of staff. The student must present valid identification such as their student card and sign this form before any data is transferred. The student name must be cross-referenced with the user id to ensure that data is not transferred into the wrong user account.
* Staff data will be transferred upon a written request from the individual. Data that is transferred between staff members will be moved only upon receipt of a written request from the user’s line manager. This does not apply to data moved by the user via their shared area.
* Extra space will be assigned to users upon request from the user or the course tutor only after all attempts have been made to archive or remove data that is not current.
* Access to shared areas will be assigned upon receipt of a written request from the shared area data owner or from the line manager.
* Access for staff members to the user areas of other staff members will only be actioned on receipt of a written request from the Head of Section.
* All requests will be stored for the audit trail.

**5. Agreement**

* Any changes that will affect the College will be made only with the full agreement of the ICT Manager and the relevant Managers.
* All changes will be made only after completion of the necessary documentation.

**APPENDIX B**

**PROTECTION AND RELEASE**

**OF STAFF OR STUDENT PERSONAL DATA**

**1. Introduction**

This code of practice aims to detail the key principles, procedures and guidelines necessary to allow for the protection of personal information retained by the College and defines the responsibilities of staff and students with regard to safeguarding personal data**. At all times staff must abide by the requirements of the General Data Protection Regulation (**Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC**).**

**2. Guarding Information and Data Protection**

There are a number of things **STAFF AND STUDENTS MUST DO**:

Make sure any personal data is,

* Kept securely.
* Fairly and lawfully processed.
* Processed for limited, stated purposes
* Adequate, relevant and not excessive
* Accurate and up to date
* Kept no longer than necessary
* Processed in accordance with the individuals’ rights
* Disposed of in an approved way, as listed by the Data Protection Officer.

Ensure that,

* Only authorised access to computers.
* Ensure that computers are locked or switched off (or logged off) when not in use - even if the work area is left temporarily.
* Make sure that unauthorised information is not obtained via a computer screen or printout (computer screens must be locked, switched off or screen savers used).

What **STAFF AND STUDENTS MUST NOT DO:**

* Remove College hardware or software from the College without prior authorisation from a member of Computer Services. Remove any personal data, electronically stored, from the College or any of its annexes.
* Remove personal data held on a computer to off-site locations unless strictly necessary for the performance of duties.
* Use any personal data for non-College or inappropriate activities.
* Disclose any personal data to third parties unless it is an exceptional circumstance covered by the Act.

**In summary staff should only handle people’s personal data in ways they would reasonably expect.**

**GUIDELINES FOR RELEASING INFORMATION ABOUT STUDENTS**

The College holds personal information about students on EBS, including name, address, date of birth, telephone number, that is covered by the General Data Protection Regulation Act and LMC staff need to ensure this information is not given out to anyone who is not entitled to receive it. However, it is also understood that maintaining good relationships with parents, carers and other agencies and keeping them informed of students’ progress is essential to securing success for many learners.

Staff have asked for some simple guidance about when they can and cannot share information to enquirers.

**GUIDANCE: GENERAL PRINCIPLES**

Please remember you cannot even say if someone is a student or not unless you know you are speaking to a secure contact.

If an enquirer is asking about a student’s attendance, progress, whereabouts etc. then:

1. Open the EBS learner file and check there is no flag on the file saying information cannot be released to anyone. If there is a flag say to the enquirer, “Sorry, I have to take advice before giving out any information” and take the enquirer’s name and telephone number. Pass the enquiry on to the Head of CIS or a Safeguarding Team member who will follow up.
2. If there is no flag then ask the enquirer who they are and then ask some ID questions that convince you that they are who they say they are: parent/carer (as named as the emergency contact) or employer for WBL. Three ID questions should be asked, e.g. student’s name, date of birth, address, telephone number. If they are not the named emergency contact or named employer then no information should be given.

If you cannot get onto EBS then you must take the enquirer’s name/telephone number and ring them back later.

If you feel in any doubt as to who they are then say, “I need to take advice” and then ring them back.

|  |  |  |
| --- | --- | --- |
| **SCENARIOS** | | **RESPONSE** |
| 1. Mother calls college requesting information whether her son attended yesterday | | * Check EBS * Check ID of caller * Release information. |
| 1. Estranged father walks into college to give student a birthday present | | * Check EBS to see if contact not barred * If OK, then seat father in Reception and ask the young person if they want to see Dad * If OK, then arrange the meeting in a supervised place. |
| 1. An employer contacts college requesting certificates for their apprentice | * Certificates belong to the apprentice, not the employer. Only release to the employer if the apprentice has given permission. | |
| 1. A solicitor contacts the college regarding the attendance and exam history regarding a former student | * The request has to come in writing and be accompanied by a signed agreement by the parent/student that it is OK to release the information. * All such requests to be dealt with by SMT, CIS or Health and Safety. | |
| 1. The Job Centre contacts the college requesting information as to whether a student is attending today | * No information to be given out except via CIS/Hayley Cody and only if it is part of our agreement/contract relating to a specific project. | |
| 1. The Job Centre contacts the college requesting information confirming that a student is studying under 16 hours per week | * No information to be given out except from the CIS office who will issue a standard letter. | |
| 1. Brother telephones to check whether their sibling is in college | * No information to be given out unless the brother is the named emergency contact and ID checks made. | |
| 1. Mother telephones stating that the granddad has been taken ill and they need to travel south to visit | * Message to be given to the student as soon as possible using the Faculty Administrator and tutors. | |
| 1. Father telephones Admissions to find out where his daughter is in the Admissions process | * Check ID and if he is the named emergency contact then issue the information. | |

|  |  |
| --- | --- |
| **SCENARIOS** | **RESPONSE** |
| 1. If someone says they are a Social Worker/Police | * Phone them back via a switchboard to check they are who they say. Do not phone back via a mobile number.   If they want information about a young person or family ask:   * Have you consent? If they have not got family consent then we need to ask the family if it is OK to share information. * The exception would be if this is a Section 47 (ie an emergency child protection issue) * Then, if they say “Yes” we can share information but we need to log all call details etc for future reference. * If it is the Police and they need information concerning a criminal investigation then we need to ask them for a DP1 (Data Protection form) * The name, address, telephone number etc of the young person is personal information and cannot be shared with anyone out of college unless it is Section 47, have a DP1 or have parental consent. |
| 1. Another college rings up asking for information on a former student | * No personal details, i.e. address, telephone number to be given out. * Academic information can be shared with care as students have given permission on the enrolment form for this. |
| 1. A support worker from a homeless agency comes into college to request copies of learner agreements for a student aged 15. He has no identification and no declaration for the student so he is sent away to get it | * The support worker comes back with a signed declaration which matches the student’s signature and ID. * Check EBS that there are no reasons why the information should not be provided then take a photocopy of the declaration and the carer’s ID badge and give him a copy of the learner agreement |
| 1. Careers teachers from local schools, academy or Local Authority contacts Marketing to ask for progression information | * If formal data sharing agreement is in place then adhere to the contract. If not, please refer to a Senior Manager for agreement of data that can be released. |

Please note: The name, address, telephone number etc. of the young person is personal information and cannot be shared with anyone out of college unless it is Section 47, have a DP1 or have parental consent.

**APPENDIX C**

**MANAGEMENT OF COMPUTER PASSWORDS**

**Student Passwords**

When students enrol at College:

* A computer account will be opened for them
* They will be given a default password which will initially be set by Computer Services.
* The password will be the student’s date of birth, formatted as follows:
  + **01Jan1980** *(please note upper and lower case characters)*.

The password must not be shared with anyone and no computer account should be used by anybody other than the person to whom it has been allocated.

When the student first logs on to a computer, they will be requested to change their password to one known only to them and the password must be:

* Unique
* At least 8 characters long
* Composed of:
  + numbers between (0 – 9)
  + upper case characters (A – Z)
  + lower case characters (a – z)
  + alpha-numeric characters (e.g. $ $ % ?)
* Contain at least one numeric character

The password:

* Can be changed only by the student or by Computer Services at the student’s request *(proof of id will be required).*

Staff may request a student’s password to be reset by emailing the Computer Helpdesk from a recognised email account.

**Staff Passwords**

When staff begin their employment at the College:

* A computer account will be opened for them
* They will be given a password which will initially be set by Computer Services.
* The password will be activated by the user creation script and will be given to the member of staff when the user id is collected *(please note upper and lower case characters)*.

This password must not be shared with anyone and no computer account should be used by anybody other than the person to whom it has been allocated.

When the staff member first logs on to a computer, they will be requested to change their password to one known only to them and the password must be:

* Unique
* At least 8 characters long
* Can include:
  + numbers between 0 – 9)
  + upper case characters (A – Z)
  + lower case characters (a – z)
  + alpha-numeric characters ( eg $ $ % ? )
* Contain at least one numeric character and one upper-case character

The password:

* Cannot be used again for at least twelve password changes
* Must be changed once every 30 days *(at automatic invitation to do so will be issued on screen).*
* Can be changed only by the staff member or by Computer Services at the request of the staff member *(proof of id will be required in person at the Computer Services Helpdesk.*

The following conditions may also apply to staff computers:

* The staff user will be allowed five password attempts before access is denied and the password will have to be reset by Computer Services.
* Screen savers will activate automatically if the machine is left idle for more than 30 minutes - Staff will then have to enter their password to deactivate the screen saver. Staff are required to manually activate this locking facility if they have to leave their computer unattended for any length of time.

**APPENDIX D**

**MANAGEMENT OF COMPUTER SYSTEMS**

**GENERIC USER ACCOUNTS**

**1. Introduction**

A generic user account will be allocated only if it is impossible for individual logon ids to be used. Typical examples are for on-line initial assessment or when visitors to the College are doing presentations.

Access on such generic logon ids is limited and no such account will have access to any Student or Staff data.

Request for a new generic user account must be made via email to the ICT Manager.

**2. Generic Accounts for Staff Use**

* Generic accounts must be reserved through Computer Services who will allocate the account to a named person.
* The account will be unlocked for the specified length of time and the authorisation sheet will be forwarded by email to the member of staff who has requested the account.
* The password is on the top of the authorisation sheet.
* Only one person can use an account at any one time so several logon ids will need to be requested for more than one visitor.
* The person using the account must sign the authorisation sheet.
* The account will be locked at the time specified in the original request.

**3. Generic Accounts for Student Use**

* Generic user accounts for students will be issued for special cases e.g. on-line assessments or taster days.
* A member of staff will reserve the account by contacting the Computer Helpdesk.
* An authorisation form will be forwarded to the member of staff who will allocate the user ids to the students.
* Individual students must sign for individual ids.
* The password is at the top of the form.
* The date and time that the id is in use must also be recorded.
* The authorisation sheet must be returned to Computer Services.
* All generic user logon ids will be locked at the end of each day.

**APPENDIX E**

**MANAGEMENT OF COMPUTER SYSTEMS USER LOGON ACCOUNTS**

**FOR STUDENTS AND STAFF WHO HAVE LEFT COLLEGE**

**1.** **Introduction**

This code of practice encompasses all computer systems that have specific user accounts created for individual members of staff and individual students.

* The list of staff who have left or are about to leave College, together with the leaving date, can be obtained from Personnel.
* Personnel provide the list weekly, as a matter of course to Computer Services, Reception, CIS, Learning Centre and Estates.
* CIS provide a report of withdrawn students. This can be run as required by the computer system’s administrator or can be obtained by contacting CIS.

**2. Procedure for Staff who have left College**

* Upon receipt of the Additions and Deletions to Telephone List all staff to be deleted will have their accounts locked and then deleted on the specified leave date.
* Any entry in the telephone list will also be deleted.
* Any account logons set up in the College’s name will also be deleted if they are known to a system administrator.

**3. Procedure for Students who have left College**

* Student accounts will be locked and deleted upon receipt of directions from a member of the college management team.
* Student accounts will be deleted during the last week in July each academic year.

**4. Generic User Accounts**

* These accounts will be deleted at the end of each academic year and will be re-created is necessary in September.

**5. Staff who are still in College employment but who are not working**

* These accounts will be locked by Computer Services upon receipt of instruction from a Senior Manager.

**APPENDIX F**

**CREATION OF STAFF AND NON-STAFF NETWORK USER ID**

All staff and visitors who use the College computer system must be issued with a valid and current user ID, which can be obtained from the Computer Services Helpdesk and fit into one of the following three categories:

**1. New staff**

* Personnel will inform Computer Services of any new staff that are due to start.
* IDs will be created and the relevant manager will be asked to confirm access requirements.
* Managers may ask Computer Services directly to create a new user ID for a member of staff by submitting a ‘Staff Network User ID Request Form’.
* Computer Services will then ask Personnel to confirm the appointment of the new member of staff before processing the form.

**2. Non-staff – 1 day presentation log on only (visiting speakers or presenters)**

* No access to network shared areas will be granted.
* Computer Services will only issue an account if they have the name of the person using the account prior to release.
* These accounts must be recorded on the ‘**Generic User Account authorisation sheet’** which should be sent to Computer Services once completed.
* The log on will be issued at the discretion of Computer Services.
* These accounts will be locked each evening.

**3. Non-staff – access to network**

* A new form - ‘Non-Staff Network User ID Request Form’ - to be completed with declarations by user and manager for Personnel to check.
* User and manager should read carefully the Safeguarding and Data Protection declarations they are signing.
* If no CRB check is in place, the manager should delete this portion of the declaration and discuss risk assessment with Personnel.
* When a form is completed, it should be sent to Personnel for checking the authorisation and date at the bottom and then it will be passed to Computer Services for processing.
* These forms will be kept on file for audit purposes.
* These accounts will have read/only (the user will not be able to edit any files on the system except those in their own personal area) access to the relevant shared areas. If Read/Write access is crucial the relevant Manager should request it through Personnel.
* Once the user ID has been created the Computer Helpdesk will contact the relevant manager so the new user can be informed that their account is now ready.

**APPENDIX G**

**STUDENT COMPUTER USE**

**1. Introduction**

Computers are provided and maintained for the benefit of all students.

Students are encouraged to use and enjoy these resources and to ensure that they remain available to all.

Any damage, malicious alteration or inappropriate use of the computer equipment may harm their education and that of other students.

To protect all in its care, the College must insist that all students adhere to its rules for acceptable use of the equipment.

**2. Help**

**STUDENTS MUST:**

* Set their password so it is **a minimum of eight characters** in length. Passwords should not be set to names or words which would be easy for someone to guess.
* Contact Computer Services on extension 265 as soon as a virus is detected by the LMC anti-virus software.

**STUDENTS MUST NOT:**

* Disclose their passwords to others or use passwords intended for the use of others

**3. Network Rules**

**STUDENTS MUST:**

* Be aware of the College **Code of Practice for e-Safety.**
* Respect, and not attempt to bypass, security in place on the computer systems. Accessing, copying removing or otherwise altering other people’s work, or attempting to alter the settings of computers is not acceptable use of the equipment.

**STUDENTS MUST NOT:**

* Store, install, or attempt to install, programmes of any type on to a computer.
* Use any utility programs or software that can monitor system activity.
* Damage, disable or otherwise harm the operation of computers, or intentionally waste limited resources.
* Use the network to harass, harm offend or insult others.
* Use the network unless they are logged on with their own ID.
* Connect any hardware devices to the College network without staff approval.

**4. Internet Rules**

**STUDENTS MUST:**

* Access the Internet only for study purposes or for College authorised activities
* Respect the work and ownership rights of people outside the College as well as students and staff. This includes abiding by copyright laws.

**STUDENTS MUST NOT:**

* Use the Internet to obtain, download, send, print, and display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.

**5. E-mail Rules**

**STUDENTS MUST:**

* Report to their tutor any unpleasant material or messages. Such reports will be treated confidentially and will help protect students.

**STUDENTS MUST NOT:**

* Give personal information such as address or telephone number to those who make contact through electronic mail.
* Send bulk mail messages (‘junk mail’ or ‘spam’ of any kind).

**6. Remote Access Rules**

**STUDENTS MUST:**

* Read the Code of Practice for Remote Access (Appendix J) before using the remote access facility.

**7. Information Security**

**STUDENTS MUST:**

* Observe and adhere to the College’s Information Security policy and the associated Codes of Practice (Appendix L and M).
* Be aware that student work (other than emails) will be backed up and archived.
* Be aware that the College is required to monitor and log user activity on all networked computer systems.

**8. Sanctions**

* Breaking of these rules will result in withdrawal of access to Information Computer Technology resources.
* Additional action may be taken by the College in line with existing practice regarding inappropriate behaviour. For serious violations, the College disciplinary procedures will be implemented.
* The College reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.
* Students must report to their tutor any security breaches. Such reports will be treated confidentially.
* Computer Services Staff will lock student user accounts immediately after instructed to do so by a member of staff or if a virus is reported by the virus checking software. The Student’s tutor will be contacted and the account will remain locked until the Tutor, having spoken to the student, instructs Computer Services in writing to re-instate the account.

**9. Monitoring**

The College has software and systems in place to record Internet usage.

Evidence from system logs will be made available to college managers upon written request.

The College reserves the right to monitor/record usage at any time. No College authorised user of the Internet should have any expectation of privacy as to his or her Internet usage.

**APPENDIX H**

**E-SAFETY FOR STAFF - KEEPING SAFE WHILST USING**

**COMPUTER SYSTEMS**

The following steps will help keep staff safe whilst using the internet.

**HELP**

**DO**

* Talk to Computer Services if you believe you have a problem with any contact made on the computer systems.
* Contact Computer Services if you need help or advice on using the computer systems or the internet in a safe way.
* Read the hints and tips about e-safety; links can be found on The Hub.
* Report cyber-bullying to your line manager
* Save any evidence / show the pages to your manager.

**INTERNET**

**DO**

* Think about keeping safe when using ICT or your mobile phone.
* Remember that you don’t know who you are in contact with - it is easy for anybody to lie about who they are online, so you can never really be sure who you are talking to.
* Type in the web address for private websites (e.g. bank account) or save it in your favourites to avoid the possibility of hacking.
* Remember that anything you post or upload to the internet is there forever so be very careful what you put online.

**DO NOT**

* Rely entirely upon technology to protect you.
* Submit personal details through an unsecured website (secure web sites have a padlock symbol on the menu bar in Internet Explorer).
* Use links from e-mail messages or websites to access web pages that ask you for personal information.
* Leave yourself logged into any site when you have finished.
* Share your passwords with anybody.
* Download software and install it on college equipment.

**SOCIAL NETWORKING AND INSTANT MESSAGING**

**(Facebook, Twitter etc.)**

**DO**

* Keep the information you submit in your profile to a bare minimum - use a pseudonym or nickname to identify yourself wherever possible.
* Avoid joining networking groups that attract negative or aggressive contributors.
* Secure your account/profile following the guidelines provided by the site provider and if you are in doubt about anything, then always seek advice.
* Bear in mind that friends of friends may not always be who they say they are.
* Use ONLY the College profiles or email accounts for College-related chat or mail.
* Always use private settings whenever you are setting up a social networking page or an Instant Messenger (IM) account. This is so that only the people who you want to see your profile can see it. Help with this can be found in the Computer Services ‘How To’ section on The Hub.
* Think about how you communicate with students - tutors must identify themselves as tutors at LMC.

**DO NOT**

* Give out any personal information about yourself online to people you do not know. This includes your full name, location, age, address, street name, postcode or work or College name.
* Give out pictures of yourself online or over a mobile, unless you know the person in real life. It is easy for people to alter your pictures and send them on or use them to pretend to be you.
* Go onto webcam with people you don’t know in real life. Webcam images can be recorded, copied and shared.
* Use personal staff accounts for contacting students or have students as ‘friends’ or in contact lists.
* Agree to meet anybody you do not know or you have spoken to online. If you do decide to meet up with anyone in real life – if you are a young person, then make sure you take a trusted adult and if you are at adult, arrange to meet in a public place at a busy time.
* If you receive any messages and pictures that worry you or upset you, talk to your line manager or report online via the website <http://www.thinkuknow.co.uk>.
* Post pictures of students onto any site without first getting guidance from Computer Services.
* Use social networking sites and web sites unless you adhere to the following criteria:
* any College related site must be approved by the Vice Principal: Finance and Resources and cleared with the Marketing Manager;
* the site should be used as a marketing medium and NOT as a student/staff discussion forum;
* any site representing the College needs to be clearly identified as such and must be held as an organisation not an individual;
* approved College sites and social accounts/pages must include the College name in the identifier;
* no pictures of staff or students are posted without prior written consent
* only appropriate content and language is used.

**MOBILE / HOME PHONES**

**DO**

* Keep personal calls to a minimum and their duration as short as possible.

**DO NOT**

* Give your mobile /home telephone numbers to students.
* Use your mobile telephone whilst teaching / assessing (except in the case of an emergency).

**VIRUSES AND MALWARE**

**DO**

* Alert Computer Services to any suspicious activity on your computer, such as pop ups, scare-ware and browser web page redirects.
* Let Computer Services know of any Anti-Virus alerts you may receive.

**DO NOT**

* Install programs on college equipment. Please contact Computer Services regarding any change in software requirements in accordance with the ICT Systems Change policy.
* Open attachments from unknown email senders. These attachments may contain malware or viruses that could damage the system. If in doubt please seek guidance from Computer Services.

**APPENDIX I**

**KEEPING SAFE WHILST USING**

**COMPUTER SYSTEMS (E-SAFETY) FOR STUDENTS**

The following steps should help keep students safe whilst using the internet.

**HELP**

**DO**

* Talk to Tutors, Programme Mentors or Computer Services if you believe you have a problem with any contact made on the computer systems.
* Contact Computer Services if you need help or advice on using the computer systems or the internet in a safe way.
* Read the hints and tips about e-safety; links can be found on The Hub.
* Report cyber-bullying or anything that you find upsetting to your tutor.
* Save any evidence / show the pages to your tutor.

**INTERNET**

**DO**

* Think about keeping safe when using ICT or your mobile phone.
* Remember that you don’t know who you are in contact with - it is easy for anybody to lie about who they are online, so you can never really be sure about who you are talking to.
* Type in the web address for private websites (e.g. bank account) or save it in your favourites to avoid the possibility of hacking.
* Remember that anything you post or upload to the internet is there forever so be very careful what you put online.

**DON’T**

* Rely entirely upon technology to protect you.
* Submit personal details through an unsecured website (secure web sites have a padlock symbol on the menu bar in Internet Explorer).
* Use links from e-mail messages or websites to access web pages that ask you for personal information.
* Leave yourself logged into any site when you have finished.
* Share your passwords with anybody.

**SOCIAL NETWORKING AND INSTANT MESSAGING**

**(Facebook, Twitter etc.)**

**DO**

* Keep the information you submit in your profile to a bare minimum - use a pseudonym or nickname to identify yourself wherever possible.
* Avoid joining networking groups that attract negative or aggressive contributors.
* Secure your account/profile following the guidelines provided by the site provider and if you are in doubt about anything, then always seek advice.
* Bear in mind that friends of friends may not always be who they say they are.
* Use the College profiles or email accounts for College-related chat or mail.
* Always use private settings whenever you are setting up a social networking page or an Instant Messenger (IM) account. This is so that only the people who you want to see your profile can see it. Help with this can be found in the Computer Services ‘How To’ section on The Hub.

**DON’T**

* Give out any personal information about yourself online to people you do not know. This includes your full name, location, age, address, street name, postcode or work or College name.
* Give out pictures of yourself online or over a mobile, unless you know the person in real life. It is easy for people to alter your pictures and send them on or use them to pretend to be you.
* Go onto webcam with people you don’t know in real life. Webcam images can be recorded, copied and shared.
* Agree to meet anybody you do not know or you have spoken to online. If you do decide to meet up with anyone in real life – if you are a young person, then make sure you take a trusted adult and if you are at adult, arrange to meet in a public place at a busy time.
* If you receive any messages and pictures that worry you or upset you, talk to your tutor or report online via the website <http://www.thinkuknow.co.uk>.
* Post pictures of other students onto any site without first getting guidance from Computer Services.

**MOBILE / HOME PHONES**

**DON’T**

* Give your mobile /home telephone numbers to anybody you do not know.

**APPENDIX J**

**REMOTE AND WIRELESS ACCESS**

**TO COLLEGE ICT SYSTEMS AND DATA**

1. **Introduction**

The purpose of this code of practice is to define standards for connecting to Lancaster & Morecambe College's network from any computer or mobile device.

These standards are designed to minimise the potential exposure to Lancaster & Morecambe College from damages, which may result from unauthorised use of Lancaster & Morecambe College resources.

Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Lancaster & Morecambe College internal systems, etc.

**2. Scope**

This code of practice applies to all Lancaster & Morecambe College employees, governors, contractors, vendors and agents with a Lancaster & Morecambe College owned or personally owned device used to connect to the Lancaster & Morecambe College Network.

This policy applies to remote access connections used to do work on behalf of

Lancaster & Morecambe College, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to:

* Dial-in modems
* Integrated Services Digital Network (ISDN)
* Digital Subscriber Line (DSL)
* Virtual Private Network (VPN)
* Secure Shell (SSH)
* Cable modems, etc.
* Web Delivered Connections (HTML5 integration, any other web delivered service)

**3. General**

3.1 It is the responsibility of Lancaster & Morecambe College employees, contractors, vendors and agents with remote access privileges to Lancaster & Morecambe College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Lancaster & Morecambe College.

3.2 Lancaster & Morecambe College employees are responsible for ensuring that they or their family members do not violate any Lancaster & Morecambe College policies, do not perform illegal activities, and does not use the access for outside business interests. Lancaster & Morecambe College employees bear responsibility for the consequences should the access be misused.

3.3 For additional information regarding Lancaster & Morecambe College's remote access connection including how to connect & troubleshooting, etc., please contact Computer Services.

**4. Requirements**

4.1 Secure remote access must be strictly controlled.

Staff and student’s passwords must meet the College’s system password criteria. ***See Appendix C Computer Password Management.***

4.2 At no time should any Lancaster & Morecambe College employee provide his or her login or email password to anyone, not even family members.

4.3 Lancaster & Morecambe College employees and contractors with remote access privileges must ensure that their Lancaster & Morecambe College-owned or personal computer or workstation, which is remotely connected to Lancaster & Morecambe College's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4.4 Lancaster & Morecambe College employees and contractors with remote access privileges to Lancaster & Morecambe College corporate network must not use non-Lancaster & Morecambe College email accounts (i.e., Hotmail, Yahoo, AOL), Social Networking Sites (i.e. Facebook, Twitter) or other external resources to conduct Lancaster & Morecambe College business, thereby ensuring that official business is never confused with personal business.

4.5 All devices, including personal ones, that are connected to Lancaster & Morecambe College internal networks via remote access technologies must use the most up-to-date anti-virus software.

4.6 Organisations or individuals who wish to implement non-standard Remote Access solutions such as contractors to the Lancaster & Morecambe College production network must obtain prior approval from Computer Services.

**APPENDIX K**

**COLLEGE INFORMATION SYSTEMS SUPPORT & MAINTENANCE**

**1. Introduction**

The support and maintenance of the College’s IT enabled information systems is one of the primary functions of Computer Services. These systems are administered by other service sections and used across college either through web interfaces or through client software.

**2. Services**

The support services for the information systems encompasses and exceeds:

* The provision, support and maintenance of an appropriate platform including servers, storage and communications technologies to meet the recommendations of the system supplier
* The provision, support and maintenance of suitable software applications and operating systems to meet the recommendations of the system supplier
* The provision, support and maintenance of a separate test environment to minimize risk to the live system
* Testing and deployment of information system software, applications and interfaces
* System and data security including disaster recover backup, testing, restoration, retrieval, storage, virus control, access control and monitoring, backup and archiving
* An understanding of current and future associated technologies to enable the strategic planning process
* A close working relationship with product technical support teams
* A close working relationship with internal application support teams
* A regular, timely set of administration and housekeeping tasks including system monitoring, capacity planning, change management, system documentation and revision/upgrade planning.

Computer Services’ change management limits risk by controlling simultaneous system updates/upgrades. In the event of co-incidental revisions being released the relevant managers will dictate the priorities.

**APPENDIX L**

**PROTECTION OF COLLEGE INFORMATION AND**

**COMMUNICATION TECHNOLOGIES**

**1. Introduction**

The acceptable use procedures and guidelines specify the actions prohibited by the College to users of the computer systems.

The aim of Lancaster & Morecambe College’s computer services, including e-mail and internet access, is to facilitate learning, communications, information access and information sharing.

The computer systems, hardware and software, are owned by the College and may be used by students to further their education and training; and by staff to enhance their professional activities, including teaching research, administration and management. Prohibited uses of the College’s computer systems procedures and guidelines have been drawn up to protect all parties; students, staff and the College.

Information Technology and other College resources exist to support the objectives of the College and should be used with this in mind.

Students and staff must report to the Data Protection Officer, all breaches of information systems security.

**Personal Use of Internet and E-mail by Staff**

* Staff may use the internet and e-mail for their own personal use out of works time provided such use is kept to a minimum
* All personal use must be within the constraints of this information security policy
* The college deploys and administers reputable spam filtering software designed to delete email spam messages that may incur a level of risk.
  1. **Access**

**YOU SHOULD:**

* Change passwords regularly. Passwords **must** be changed every thirty days by staff.
* Lock all doors and windows when leaving a room.
* Keep keys for computer rooms and safes in a secure place.

**YOU SHOULD NOT:**

* Leave portable computers and storage devices in places where a thief can easily steal them; specifically laptops, PDAs, removable storage, external hard drives, CD/DVD media and pen drives.
* Try to mend any IT equipment yourself – always get help.
* Move any fixed ICT equipment without first consulting the Computer Services Helpdesk.
* Trail cables to create a trip hazard.
* Place a computer right next to radiators, water pipes or other sources of heat or damp.
* Allow unauthorised access to computer hardware, software and data. Eligible users are employees of Lancaster & Morecambe College, members of the Lancaster & Morecambe College Corporation, currently enrolled students of Lancaster & Morecambe College and third party individuals or organisations approved by Lancaster & Morecambe College.
* Disclose passwords to others or use passwords intended for use by others.
* Allow unauthorised access by students and staff to secure areas (Finance, Personnel, Staff offices, College information systems and Computer Services).
* Allow unauthorised access to dial-in facilities by external suppliers.
* Allow students in rooms with computers without a member of staff being present.
  1. **Software & Data**

**YOU SHOULD:**

* Save copies of your data regularly.
* Get rid of documents you don’t need anymore.
* Save all files to the network before copying them to external media such as pen drives or disks.
* Take all software to the Computer Services Helpdesk for checking prior to using it in any College computer.
* Follow the software procurement policy which is that all college software assets must be purchased via the ICT Manager.

**YOU SHOULD NOT:**

* Assume that your backups will work automatically.
* Leave disks or pen drives next to your computer. Use storage boxes and lock them away or they could be stolen with the computer itself.
* Use software for non-educational purposes. Permitted uses include teaching, research, administration and management of the College’s organisation.
* Copy College software.
* Copy or use one’s own software, including games on any College computer. Failure to comply may result in the transmission of viruses.
* Purchase college software assets directly without the approval of the ICT Manager.
  1. **Network**

**YOU SHOULD:**

* Install all hardware and software onto the College computer systems **only after** **authorisation** by the ICT Manager.
* Save only confidential files into personal home folders.
* Save files that are not considered to be confidential into the staff shared area.
* Lock or log-off any computer you leave unattended.

**YOU SHOULD NOT:**

* Damage, disable or otherwise harm the operation of computers, or intentionally waste limited resources.
* Use the network for commercial purposes, for example, buying or selling goods or services and advertising.
* Use the network in such a way that harasses, harms, offends or insults others.
* Bypass security on the computer systems.
* Hack or engage in other deliberately disruptive activities.
* Access, copy, remove or otherwise alter other people’s work, or attempt to alter the setting of computers.
* Create, configure or adopt external web sites or other on-line areas for the delivery or storage of any College-related information.
* Install unauthorised hardware or software.
* Change the settings or the configuration of any of the College’s Information and Communication Technology
* Alter or interfere with the network infrastructure including cabling, trunking, power, data, wireless, telecoms, audio visual equipment, routers, switches or ports.
  1. **Internet**

**YOU SHOULD:**

* Respect the work and ownership rights of people outside the College and abide by copyright laws.
* Check all downloaded files for viruses **before** use.

**YOU SHOULD NOT:**

* Use the internet for any purpose that may bring the College into disrepute or cause offence to other people.
* Access the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, offensive, obscene, racist, pornographic or abusive.
* Disclose personal information such as addresses, telephone numbers or photographs to those only met through the internet.
* Engage in chat activities over the internet. This takes up valuable resources, which could be used by other people.
* Use the internet for commercial purposes, for example, selling goods or services or advertising.
* Create any College-related web sites or subscribe to third-party web sites in the name of the College without first consulting Computer Services and Marketing.
  1. **E-mail**

**YOU SHOULD:**

* Take individual responsibility for all e-mail sent and for contacts made that may result in e-mail being received.
* Use the same levels of language and content for e-mails as for letters or other media.
* Check e-mail attachments for viruses before use.
* Save any email or attachment to the network if you wish to keep it.

**YOU SHOULD NOT:**

* Send bulk mail messages (‘junk’ mail or ‘spam’) of any kind.
* Disclose personal information such as photographs, addresses or telephone numbers to those only met through e-mail.
* Use e-mail for commercial purposes.
* Expect emails to be automatically backed up.
* Expect emails to be saved to the network automatically.
* Attach large or zipped files to email messages.
* Keep any unnecessary emails.
  1. **Viruses**

**YOU SHOULD:**

* Ensure that any storage media coming into the College, no matter where it has come from, is checked for viruses.
* Make sure that virus checking software is used.

**YOU SHOULD NOT:**

* Use any non-College software including screensavers, free disks, public domain software or demonstration software.
  1. **Portable (Laptop) computers**

**YOU SHOULD:**

* Store portable computers securely when not in use.
* Use password protected screensavers.
* Use anti-virus software.
* Virus check external media prior to use.
* Report any stolen portable computers to the College.

**YOU SHOULD NOT:**

* Leave portable computers in places where a thief can easily steal them.
* Leave portable computers in an unattended car.
* Install unauthorised software or download software/date from the Internet.
* Plug any laptop into the College network.
  1. **Wireless Network Connection**

**YOU SHOULD:**

* Always ask Computer Services if you are unsure.
* Follow the instructions provided by Computer Services.
* Utilise a personal firewall.
* Ensure that the operating system is fully patched and running the latest service pack.
* Adhere to the associated college policies and procedures when using the college wireless network

**YOU SHOULD NOT:**

* Send, receive or make available any material that might be considered offensive, obscene or indecent.
* Send, receive or make available any material that might infringe copyright, e.g. MP3 or other audio and video formats.
* Run peer-to-peer (P2P) file sharing software.
* Intercept or attempt to intercept other wireless transmissions.
* Access or run utilities or services as these might negatively impact on the overall performance of the network or deny access to the network, harass, cause annoyance, nuisance or inconvenience to others.
* Access or attempt to access systems or resources to which you are not authorised.
* Provide services which may interfere with normal network operation.
* Provide access to others, e.g. allowing a third party to use your credentials to access the network.
* Change settings or configuration of any of the College’s Information and Communication Technology.
  1. **Monitoring**

The College gathers log information from users’ web access requests to ensure compliance with:

* Web sites or content that have child protection of safeguarding implications
* Access within the parameters of the JaNet acceptable use policy

**APPENDIX M**

**SECURITY BACKUP OF COLLEGE DATA**

**1. Introduction**

Data is an important asset of the College and data backup involves the storing of files from the College computer network in another location.

In this way, if there is ever any loss of data on the live system, the College will still have that data in backup in order to restore files.

This document defines the minimum requirement for the security archiving and restoring of College data.

**2. Dependencies**

* Tape Library System
* Backup Software
* LTO Tapes to store up to 400Gbytes (uncompressed
* 800Gbytes (compressed)
* Fire proof safes to two locations
* Maintenance cover on Tape Library System.

**3. Backup Procedure**

**3.1 Full disaster recovery**

* ~~D~~isaster recovery backups to be taken during each term **and half term breaks.**
* For any changes to the server settings where a snapshot isn’t available for virtual servers.

**3.2 Weekly backup**

* One full weekly backup of all data areas to be taken over each weekend of the month.
* Fire Proof Safe at main site and a copy sent to Morecambe Learning Centre.
* The tapes will be rotated on a monthly basis with the FULL backup for the last Saturday of each month archived in the fire proof safe in Morecambe Learning Centre.

**3.3 Incremental Backup**

* An incremental backup of all data to be taken each weekday night Monday to Thursday inclusive.
* Each evening will be allocated specific tapes on a weekly basis, rotated on a monthly basis.
* Backup tapes will be copied and stored in separate areas.
* Copies will be stored in fire-proof conditions.

**3.4 Full System Archive Backup**

* A full system archive backup to be created annually on the last Saturday in July.
* These tapes will be stored for up to forty years or for such a time and in such conditions as to meet the College’s mandatory regulatory requirements.
* The backup system will automatically log the following information:
* Start date
* Start time
* Successful (or not)
* End date
* End time
* The date the tape was commissioned

**4. Restore Procedure**

* Restores, wherever possible, will be made using a weekday tape.
* The most recent successful backup tape will be used.
* If the data is not available on a weekday tape, the monthly tape will be retrieved from Firesafe1 and will be used.
* On a monthly basis weekly tapes will be tested for successful restore using three test restore files on the tapes for each individual weekday.
* All restores must have a formal written request.
* The test restore of the most recent monthly archive tape will be undertaken on the Wednesday following the backup.
* The disaster recovery system will be tested within seven days of the latest disaster recovery tapes being made – whenever practical (allowing for college closures).
* Restored data files will be delivered to the user within 4 working days.
* The file name, owner, date of restore, time of restore and success will be logged on a restore log sheet in the electronic form submitted by the requester.
* Prior to the restoration of data a data restore form must be completed (can be found in the forms section of the hub).

**5. Servers to be Backed-up**

A full schedule is available from Computer Services.



**Initial Screening for Equality Impact Assessment (including Safeguarding)**

*To be completed prior to a Policy, Procedure being introduced/renewed.*

**PART ONE: INITIAL SCREENING**

|  |  |
| --- | --- |
| **Name of policy/Plan/Procedure being assessed:**  **IT Policies, Procedures and Guidance**  **Is this a new or existing policy/function?**  Existing ÖNew  **□** | **Name of manager/group carrying out the assessment:**  **Jonny Wright – ICT Manager** |
| 1. **In which of the listed areas could the new/amended policy, plan or procedure have an impact?**   These areas follow the College SES  NB: This could be positive as well as negative.  (please tick box) | Ö Gender ÖRace and Ethnicity  Ö Disability ÖSexual Orientation  ÖAge ÖReligion/belief  ÖSocio-Economic **□** Pregnancy/Maternity  **□** Gender Reassignment  **□** None expected  **□** Marriage/Civil Partnership |
| 1. **What are the risks of introducing this change to any of the above groups?** | None |
| 1. **What are the expected benefits of introducing this change to any of the above groups?** | The strategy specifically addresses the contribution of the Computer Services Department to the College Safeguarding Agenda |
| 1. **Are there any areas or issues that could impact on the safety of staff or learners?** | eSafety through internet access  unauthorised access to personal data |
| 1. **What evidence do you have for the listed areas.** | Prevent Strategy  Safeguarding policy  GDPR |
| 1. **Is this policy/plan/procedure deemed to have a of High, Medium or Low risk?** | Low |
| 1. **Is there any further action to be taken as a result of completing this screening form?**   *For example, a need to complete a full Equality Impact Assessment or to set the date of a review.* | **Is a full screening Impact Assessment required?**  Yes **□** No Ö  If yes, please move to complete Part 2 overleaf  **Date of review: 08/03/2020** |
| **Signed (completing Officer)**  Jonny Wright  **Job Title: ICT Manager** | **Date of completion of Impact Assessment:**  08/03/2019 |

***This document should be securely stored with the relevant policy/procedure***