Painsley Catholic College

ICT Security Policy
2023-2024

Index

Appendices

Foreword

The Board of Directors of Painsley Catholic College is required under Financial Regulations to formally approve and implement an ICT Security Policy that complies with the County Council's minimum standards on computer security.

This "ICT Security Policy" has been modified by Painsley Catholic College from a model by the County Council, reviewed by LMSCC.

Corporate and individual responsibilities are clearly defined within the policy. The Principal formally nominates Mr M. Palmer (Assistant Principal) to carry out these responsibilities. There are also procedural and functional aspects of the policy that the College must action in order to implement the policy. These are presented in Appendix B2 of the policy. On of the key procedural aspects is the distribution of rules and agreements for the ICT users that outlines their responsibilities under the ICT Security Policy. These acceptable "rules for ICT Users" are presented as Appendix C1-C3. A strategy on the "backup" of data is attached as Appendix B3. Appendix B4 contains details of security guidelines to assist the Network Manager in his role.

The 'model' also includes an Acceptable Use Policy (Appendix A). This refers to the Acceptable Use of ICT Equipment for Staff and Pupil use, and Third Parties, (Appendices C1 – C3) which all users need to agree to as an integral part of the ICT Security Policy. All users must complete the relevant consent or declaration form if they want to use the facilities.

Information and Communications Technology (ICT) Security Policy

1. Introduction

1.1 We are managing a significant investment in the use of ICT. In many areas of work the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data be maintained at a level that is appropriate for the College's needs.

1.2 Sufficient resources should be allocated each year to ensure the security of the College's ICT systems and to enable users to comply fully with the legal requirements and policies covered herein. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to directors.

2. Policy Objectives

2.1 Against this background there are three main objectives of the ICT Security Policy:-

a) To ensure that equipment, data, staff and students are adequately protected on a cost effective basis against any action that could adversely affect the College;

b) To ensure that users are aware of and fully comply with all relevant legislation;

c) To create and maintain within the College a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

2.2 If difficulties arise in the interpretation and/or appreciation of any aspects of the Policy, the ICT Support Team within the College should be consulted.

3. Application

3.1 The ICT Security Policy is intended for all College staff that have control over, use or support the College's administration and curriculum ICT systems or data. Pupils using the College's ICT systems or data are covered by the relevant "Acceptable Use Policy" documents, which are incorporated within document.

3.2 For the purposes of this document the terms 'ICT' (or 'ICT system'), 'ICT data' and 'ICT user' are defined as follows:-

- 'ICT' (or 'ICT system') means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held portable device, tablet, notebook, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system or any other similar device;

- 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound;

- 'ICT user' applies to any Painsley Catholic College employee, pupil or other authorised person who wishes to use the College's ICT systems and/or data.

4. Scheme of Delegation under the ICT Security Policy

4.1 The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are clearly defined below.

4.2 Owner

4.2.1 The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the College are the legal property of the College.

Exceptions to this will be allowed for software and documentation produced by individual teachers for lesson purposes – this includes schemes of work, lesson plans, worksheets or as otherwise agreed in writing by the Principal.

4.2.2 We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

4.3 Board of Directors

4.3.1 The Board of Directors has ultimate corporate responsibility for ensuring that the College complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.

In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Principal.

4.4 Principal

4.4.1 The Principal is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the College's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the College. He/she is also responsible for ensuring that any special

ICT security measures relating to the College's ICT facilities are applied and documented as an integral part of the Policy.

In practice, the day-to-day functions should be delegated to the 'Network Manager', who must be nominated in writing by the Principal (see Network Manager job description).

4.4.2 The Principal is also responsible for ensuring that the requirements of the Data Protection Act 2018 are complied with fully by the College. This is represented by an on-going responsibility for ensuring that the :-

- registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and
- registrations are observed within the College.

4.4.3 In addition, the Principal is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and portable devices at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 2018.

4.5 The Assistant Principal (with responsibility for ICT)

4.5.1 The Assistant Principal (with responsibility for ICT) is responsible for the implementation of the College's ICT Policy. The Assistant Principal (with responsibility for ICT) for the purpose of this policy will be known as the IT manager. The IT Manager may appoint competent persons to carry out practical implementation of the College's policy.

4.6 Network Manager

4.6.1 The 'Network Manager' is responsible for the College's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The Network Manager will be an employee of the College or the County Council.

Some of the additional work will be carried out by Staffordshire ICT Department. Within the College the Network Manager will carry out day-to-day duties.

4.6.2 Consequently, the Network Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

4.6.3 In line with these responsibilities, the Network Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Principal or Chair of Directors of any suspected or actual breach of ICT security occurring within the College. The Principal or Chair of

Directors should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Principal or Chair of Directors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity. Details of suspected or actual breaches are recorded by the Network Manager in to the 'staff.mdb'. The breeches by students and other parties are recorded into the student security database.

4.6.4 It is vital, therefore, that the Network Manager is fully conversant with the ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

4.7 Internal Audit

4.7.1 The County Council's Internal Audit Section is responsible for checking periodically that the measures prescribed in each College's approved ICT Security Policy are complied with, and for investigating any suspected or actual breaches of ICT security.

4.7.2 Specialist advice and information on ICT security may be obtained from the County Council's ICT Unit, who will liaise with Internal Audit on such matters.

4.8 Users

4.8.1 All users of the College's ICT systems and data must comply with the requirements of this ICT Security Policy, the relevant rules of which are summarised in *`The Rules for ICT Users'* attached in Appendix C.

4.8.2 Users are responsible for notifying the Network Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Principal, Chair of Directors or to Internal Audit.

5. The Legislation

5.1 Background

5.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of :-

GDPR/Data Protection Acts 1984, 1998 & 2018;

Computer Misuse Act 1990;

Copyright, Designs and Patents Act 1988

The Telecommunications Act 1984

5.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

5.1.3 The general requirements arising from these acts are described below.

5.2 GDPR/Data Protection Acts 1984, 1998 & 2018

5.2.1 GDPR/The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Principal is required to compile a census of data giving details and usage of all relevant personal data held on computer within the College, and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation.

5.2.2 Users of personal data are aware of, necessary legislation before they are given access to our systems. Periodically staff have access to updated copies of the ICT Staff handbook via the College VLE which include information about the relevant Acts.

5.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.2.3 Further information on the College's policy regarding personal data can be found in the "Painsley Catholic College Personal Data Policy"

5.3 Computer Misuse Act 1990

5.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-

Unauthorised access to a computer system or data;

Unauthorised access preparatory to another criminal action;

Unauthorised modification of a computer system or data.

5.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of College policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4 Copyright, Designs and Patents Act 1988

5.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

5.4.2 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

5.4.3 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

5.4.4 The Network Manager is responsible for compiling and maintaining an inventory of all software held by the College and for checking it at least annually to ensure that software licences accord with installations. To ensure that we comply with the Copyright, Designs and Patents Act 1988 and in order to satisfy the County Council's responsibilities as a corporate member of FAST (Federation Against Software Theft). Users are not allowed copies of any software purchased by the College unless the particular licence allows it.

5.4.6 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of College policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

5.5 The Telecommunications Act 1984 and 2000

5.5.1 The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.

5.5.2 The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

6. Management of the Policy

6.1 The Principal should allocate sufficient resources each year to ensure the security of the College's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Directors.

6.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data (see ICT staff handbook). A record of the training provided through the College to each individual user will be maintained in the Staff Training Database.

6.3 In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security. (see IT Staff Handbook and Personal Data Policy)

6.4 To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users. (see IT Staff Handbook)

6.5 The Principal must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:-

- A record that new staff have been issued with and have read the appropriate documentation relating to ICT security, and have signed the list of rules;

- A record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;

- A record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment;

7. Physical Security

7.1 Location Access

7.1.1 Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to

rooms that contain servers or provide access to data. The Server Room, when unattended should be permanently locked by key.

7.1.2 The Network Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

7.2 Equipment siting

7.2.1 Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:-

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;

- equipment is sited to avoid environmental damage from causes such as dust & heat;

- users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users; (see Acceptable Use Policy)

- users have been instructed not to leave hard copies of sensitive data unattended on desks; **The same rules apply to official equipment in use at a user's home.**

7.3 Inventory

7.3.1 The Principal, in accordance with the College's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually.

8. System Security

Appendix B6 contains details of security guidelines for Network Managers.

8.1 Legitimate Use

8.1.1 The College's ICT facilities must not be used in any way that breaks the law or breaches County Council standards.

Such breaches include, but are not limited to:-

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorised private use of the College's computer facilities.

8.2 Private Hardware & Software

8.2.1 Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the College's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The Network Manager must approve the use of all private hardware for College purposes. (see hardware/software request form).

8.3 ICT Security Facilities

8.3.1 The College's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 8. The College makes use of RM Auditor for tracking and monitoring of network use by individuals and groups of users.

8.4 Authorisation

8.4.1 Only persons authorised in writing by the Network Manager, are allowed to use the College's ICT systems. The authority given to use a system will be sufficient but not excessive and the authority given must not be exceeded.

All ICT systems on logon display a message to users warning against unauthorised use of the system.

8.4.2 Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the College. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

8.5 Access to the County Council Corporate ICT Network

8.5.1 The Principal must seek permission on behalf of the College for any ICT system to be linked to the County Council's corporate ICT network.

In the College environment this applies to the access granted in Colleges to the County Council's systems for financial, payroll and creditor payments purposes. These facilities may well be extended to other areas of operation and functions of the County Council.

8.6 Passwords

8.6.1 The level of password control will be defined by the Network Manager based on the value and sensitivity of the data involved, including the possible use of "time out" passwords where a terminal/PC is left unused for a defined period.

8.6.2 Passwords for staff users should be changed at least termly and should not be re-used. They should be a minimum of 8 alphanumeric characters, mixed case, mixture of letters, symbols and numbers and not obviously guessable.

8.6.3 Passwords should be memorised. If an infrequently used password is written down it should be stored securely.

Passwords and screen saver protection should protect access to all ICT systems, particularly portable device/notebook/tablet PCs as they are highly portable and less physically secure.

8.6.4 A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:-

- When a password holder leaves the College or is transferred to another post;
- When a person may knows a password that they are not entitled to.

The need to change one or more passwords will be determined by the risk of the security breach.

8.6.5 Users must not reveal their password to anyone, apart from ICT support staff. Users who forget their password must request the Network Manager issue a new password.

8.6.6 Where a password to boot a PC or access an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network.

8.6.7 System passwords (systemadmin, administrator, pweston, aread) are changed every 2 months. Policy and procedures are stored in the IT Support safe and with Mrs Bradbury as is a Red Bus Policy in case of emergencies where Mr Read or Mr Weston are unable/unavailable to manage the network, this includes a sealed signed envelope of passwords.

8.7 Backups

8.7.1 In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the Network Manager, dependent upon the importance and quantity of the data concerned.

The backup strategy for Painsley Catholic College is presented at Appendix A3.

Where programs and data are held on other systems not connected to the Painsley Catholic College Network, e.g. portable devices the user will normally need to make security copies of their data.

8.7.2 Security copies are clearly marked in a rotational system. The curriculum network tapes are stored in a fireproof locked safe in the ICT Office. The admin network backups are stored away from the server in the Admin Officer's office. The Network Manager takes the Friday backup of the curriculum and admin networks off site every Monday; in accordance with the Data Protection Act the College has a written record of where the off site backup is kept. (this is kept with the principal)

8.7.3 Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be reloaded in cases of system failure.

8.8 Virus Protection

8.8.1 The College will use appropriate Anti-virus software for all College ICT systems.

Colleges are actively encouraged to conform to the recommended anti-virus protection standards. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

8.8.2 The College will ensure that every ICT user is aware that any PC with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the Network Manager who must take appropriate action, including removing the source of infection.

The Board of Directors could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on College equipment.

8.8.3 Any third-party portable devices not normally connected to the College network must be checked by the Network Manager for viruses and anti-virus software before being allowed to connect to the network.

8.8.4 Teachers must take the necessary steps to ensure anti-virus protection software on their portable device is updated on a weekly basis as a minimum.

8.9 Disposal of Waste

8.9.1 Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived. Any Computer that is disposed of must have its hard drive destroyed before removal.

The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

8.10 Disposal of Equipment

Prior to the transfer or disposal of any ICT equipment the Network Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data,

they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

The Data Protection Act requires that any personal data held on such a machine be destroyed.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

8.11 Repair of Equipment

8.11.1 If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored other media for subsequent reinstallation, if possible. The

College will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as College staff in relation to not divulging the data or making any unauthorised use of it.

9 Security Incidents

9.1 All suspected or actual breaches of ICT security shall be reported to the Network Manager or the Principal in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly. Security incidents are logged in the same database as those incidents logged regarding e-safety.

The Audit Commission's Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

It should be recognised that the College and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the College where insufficient action had been taken to resolve the breach.

10. Acceptable Use Policy

10.1 Attached as Appendix A is the "Acceptable Use Policy". This policy applies to all College staff, students and third parties who use either or both of these facilities. The conditions of use are explained in the policy. All College staff and visitors accessing these facilities must be issued with a copy of the 'Acceptable Use Policy – Staff and Third Parties' document and complete the user declaration attached to the policy. For all students, the College will ensure that the relevant 'Acceptable Use Policy - Students' document is issued and the consent form is completed by pupils and their parents. All of these documents are contained in Appendix C.

APPENDIX A1

Implementation Program

Painsley Catholic College will adopt the ICT Security Policy consisting of the following:

Whole College

- ICT Security policy for Colleges – (Completed)
- Board of Directors and Principal to implement procedural aspects of policy - follow requirements detailed in LEA 'model' policy in **Appendix A2.** (Completed)
- Backup strategy – **Appendix A3.** (Completed)
- Hardware inventory – Central Database is currently in place and maintained
- Software inventory – Central Database is currently in place and maintained
- Security guidelines – **Appendix A4 guidelines are followed** (Completed)

For Staff and Third Parties

- Acceptable Use policy for staff and Third Parties– Adapted from LEA Guidelines to own security needs **Appendix B1.** (In place)
- Staff/Third Parties declaration form – All Staff to sign, filed away and recorded as signed **Appendix B1.** (In place)

For Students

- Acceptable Use policy – recommended policy included in LEA 'model' policy as **Appendix B2.** (In place)
- Pupil / Parent consent form – Permission slips adapted from LEA Model **Appendix B2.** (In place)

Each of these documents (overleaf) will need to be reviewed on a regular basis. Completing the following table will document the policies adopted by the College and assist in identifying the relevant review process. Any other implementation issues can also be documented in the following section.

Documents relating to ICT Security Policy for Colleges

Document Name	Model document used or Colleges own version?	Location of Document	Produced / Reviewed By	Last Review Date	Date next Review is due
ICT Security Policy	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Procedural Aspects (Annex B2)	Own	ICT Office	M Palmer	Jan 2023	Jan 2024

Backup Strategy (Annex B3)	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Hardware Inventory	Own	Database	M Palmer	Jan 2023	Jan 2024
Software Inventory	Own	Database	M Palmer	Jan 2023	Jan 2024
Security Guidelines (Annex B6)	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Rules for ICT Users – Staff and Third Parites (Annex C1)	Model	ICT Office	M Palmer	Jan 2023	Jan 2024
Acceptable Use Policy – Staff and Third Parties	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Declaration form for Staff (Annex C1)	Model	ICT Office	M Palmer	Jan 2023	Jan 2024
Acceptable Use Policy -Students (Annex C2)	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Pupil / Parent Consent Form (Annex C2)	Model	ICT Office	M Palmer	Jan 2023	Jan 2024
E-safety Policy (Annex Nn)	Model	ICT Office	M Palmer	Jan 2023	Jan 2024
Personal Data Policy (Annex Nn)	Model	ICT Office	M Palmer	Jan 2023	Jan 2024

Communications Policy	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Filtering Policy	Own	ICT Office	M Palmer	Jan 2023	Jan 2024
Response to Incidents Policy	Model	ICT Office	M Palmer	Jan 2023	Jan 2024
Use of Digital Images and Videos Policy	Own	ICT Office	M Palmer	Jan 2023	Jan 2024

Nominated ICT Manager: M Palmer

Nominated Network Manager: Mr T. Szabunia

APPENDIX A2

Procedural Aspects of the Policy

1. The **Board of Directors** must ensure that the College implements an ICT Security Policy - this can either be the 'model' policy or the College can create an amended policy based upon the 'model'. This must be reviewed annually and must include Acceptable Use Policies for Staff and Pupils

2. The **Principal** must nominate a Network Manager or members of non-teaching staff with designated systems management responsibilities. This is documented (*in Appendix A1 of the policy*) and included in the Scheme of Delegation approved by the Board of Directors.

   The Principal must ensure that the nominated member(s) of non-teaching staff understands the functions of the role and is familiar with the relevant Acts

3. The **Principal** must compile a census of data giving details and usage of all personal data held on computer and manually (as required under the Data Protection Act 1998) in the College, and file a registration with the Data Protection Registrar.

   Users should be periodically reminded of the requirements of the Data Protection Act, particularly the limitations on the storage and disclosure of information.

4. The **Principal** should ensure that a copy of the relevant 'Acceptable Use Policy' (*attached as Appendix B1-B2*) is issued to all system users. This should include all relevant aspects of the ICT Security Policy and any other information on the use of facilities and techniques to protect the systems or data.

   This will include

   - Inappropriate use of Email and the Internet
   - Breaches of security - reporting procedures
   - Use of private hardware and software
   - User authorisation process
   - Access rights
   - Appropriate use of the College facilities
   - E-safety
   - Personal data
   - Use of Digital and Video Images
   - Communications
   - Filtering

5. The **Principal** or nominated person should retain a record of

- the distribution of the 'Acceptable Use Policy' - to Staff, Students and third parties;
- the access rights to systems and data granted to individual users;
- any amendments or withdrawal of these rights due to a change in responsibilities or termination of employment or starters/leavers;
- the training provided to each individual user.

6. An inventory of all ICT equipment must be maintained and regularly updated by the person appointed by the **Principal** ie Network Manager as equipment is purchased / disposed of. The inventory must be checked and verified annually in accordance with the requirements of Financial Regulations.
(*Done as a database and stored by the ICT Department*)

7. The **Principal** should define local rules regarding the use of privately acquired hardware and software, which should be disseminated to all Users. This will also include use of non-approved email accounts.

8. An inventory of all software and licence details must be maintained and regularly updated by the **Network Manager** as software is purchased / disposed of. The inventory must be checked annually to ensure that the licences accord with installations. *(Done in a Database and Stored by the IT Department)*

The Network Manager should ensure there are clear procedures regarding the installing / copying of software. The Network Manager should be familiar with the requirements of FAST (the Federation Against Software Theft)

9. The **Network Manager** should ensure there are clear procedures regarding installing, upgrading, repairing and disposal of equipment.

10. The **Network Manager** must decide on the appropriate frequency for password changes and advise on the technique for password selection based on the value and sensitivity of the data involved, and advise users accordingly.

The Network Manager must ensure there are clear procedures regarding the disposal of equipment and waste containing confidential or sensitive data.

11. The **Network Manager** must ensure that a Backup strategy is agreed, documented and implemented. Clear instructions must be given to Users to ensure this is followed. *(See Appendix A3)*

12. The **Network Manager** should confirm and implement a policy on anti-virus software for local networks, standalone systems, portable devices, home PC's and remote devices such as telephones, PDAs and notebooks. (particularly where data may be transferred to College). This must ensure that anti-virus software is regularly updated.

13. The **Network Manager** must distribute the "Acceptable Use Policy" (*Appendix C*) to all Users and ensure that they complete the relevant User declaration attached to the policy.

APPENDIX A3

Backup Strategy

- All Data held on the administration and curriculum networks will be backed up daily, on each day of the working week. This will ensure that at least five copies of data are always available.
- A four-week backup rotation of Friday tapes exists on the curriculum network. A two-week backup rotation exists of Friday tapes for the Administration network.
- All backups should be checked regularly to ensure they have been successful (e.g. If a backup has been made to a tape, the contents of the tape should be checked to see that a file exist and can be restored)
- A "Long Term Backup" Will be taken at the beginning of each term. This will be kept and not overwritten until the beginning of the next term. This will help protect against data corruption that goes un-noticed for several weeks, during which 'newer' backups will have overwritten 'older' ones.
- A backup of the system will be taken before any major system changes take place
- A Backup of a "clean system" will be taken when the system is first set up

APPENDIX A4

Security Guidelines

1. Password Policy

Within Painsley Catholic College, the policy for passwords on the network is as follows:

Passwords should be:

- Unique
- Alphanumeric
- At least 6 digits in length
- Regularly Changed, (where practicable).

Passwords should not be

- Written Down
- Easy to guess
- Distributed to any other members of staff

2. Monitoring Computer use by Pupils

Students should not be allowed into ICT Rooms without correct supervision, this should be in the form of an ICT Supervisor or a member of staff. Where an ICT Supervisor is present a member of staff must be available to deal with any unforeseen circumstances.

When students are on the network, their actions can be monitored via Impero and PCE. This is to police the correct use of the network and the internet.

All rooms will be laid out in order for staff to have good visibility of computer screens, if this is not possible, then training in Impero will be offered as a backup monitoring tool.

All students will be randomly subject to auditing of printing, web access and work areas using various audit tools anything found to be unsatisfactory will be removed without prior consultation and may be subject to disciplinary action.

3. Monitoring Computer use by staff

Staff on the admin network will be trained in the use of screen saver passwords and must be expected to apply these on leaving a station.

Any equipment used to display sensitive information (i.e. Student information), should be shielded from unrestricted access.

Any printouts that contain sensitive information should be disposed of in a careful manner.

4. System Backup

The Curriculum and admin networks will be backed using the backup policy as stated in Appendix A3.

5. Anti Virus Protection

The College is protected by Symantec Antivirus on the curriculum and administration networks. This will update automatically from the servers and the Internet.

Portable devices are all set up with Symantec anti-virus protection. Portable devices should be logged on regularly to ensure that anti-virus protection is kept up to date.

Any attempt to interfere with the anti-virus software or maliciously bring in a virus to the College will be met with extreme penalties.

6. Illegal or Inappropriate use of the network

- Passwords control access the network, do not share your password with anyone.
- Work areas will be periodically swept for inappropriate material; any material found of an unsuitable nature will be removed without consultation.
- Access and usage statistics will be produced and monitored via RM Auditor in order to track the usage of files on the network.
- The network is protected and filtered by a proxy server and firewall to restrict access to inappropriate material and to prevent inappropriate external access

7. Internet Use/Filtering

- Internet filtering is done via smart cache 2.
- There are acceptable use policies for each group of users; Staff, Students, Third Parties (See the relevant section in the security policy for details). All members of the College must sign an acceptable use policy on starting the College.
- Parents are asked to sign the acceptable use policy so that they agree with the terms laid out in the AUP
- Should any inappropriate material be found, the finder must report the Website immediately to the Network Manager, in order to avoid ramifications directed towards them.
- Executable files are not allowed to be downloaded or run on the network.
- All Internet use is supervised as laid out in section 2.

8. E-Mail use

- The College has adopted an e-mail policy for all its members and it is documented in the acceptable use policy given to every person on arrival at Painsley.
- Current inbox size is set to 9Mb with a maximum of 4Mb for an e-mail.
- The College will not tolerate abusive e-mails to any other person inside or outside the College.
- E-Mail's will be closely monitored for such breaches of security and SPAM

9. Personal Data

- See Personal Data policy.

10. Documentation

- Procedures for Building Machines, adding and removing members of staff/students and setting up portable devices are all presented in Tick sheet form in the IT Office.
- Housekeeping procedures are also laid out in the Housekeeping Document.
- Backups are all kept in the Safe, with the Friday backup for admin and curriculum networks being taken off site with the Network Manager.

11. Training

- Adequate training for Network Managers and Users is provided.
- Induction ICT training for new staff takes place soon after they start work.

12. Authentication / Operating system level security

- Use system policies to provide additional security
- There is a rigorous policy for approval/removal of users (Tick sheets)
- The use of generic accounts is avoided.
- The number of administrator and manager accounts is strictly limited.
- The use of groups with administrator or manager rights is avoided.
- Clear security levels are set on the network and ensure these are documented and followed
- There is restricted access to applications and data areas where appropriate
- Use is made of "read only" access where possible
- Where possible only log on as a system administrator in the IT Office

13. Network Review

- Disaster Recovery: Should a server go down, Staffordshire county council has a server response team that respond to critical failure within 30 minutes.
- All faults logged with the system are responded to within the time limits laid out in the IT Service Desk Policy. This is monitored in order to pursue an IT Quality of Service
- The IT Security, Housekeeping and other official documents should be reviewed every year.
- Regularly review appropriate documents e.g. computer security policy and acceptable use policy.
- Review procedures for dealing with all the security breaches or compromises, whether deliberate or innocent.

14. Monitoring systems usage

- Monitoring of data on a College network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the College's day-to-day activities.
- A College may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Painsley will ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.
- The Rules for Email and Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the College is monitoring use.
- In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, Painsley has procedures for monitoring. The ICT manager supervises monitoring and the maintenance of a log of that monitoring.

APPENDIX B0

Information and Communication Technology

Acceptable Use Policy –Staff and Third Parties

1. Do not disclose password information to anyone unless authorised to do so by the Information Technology (IT) Technical Team.
2. Do not allow other persons to use systems that you have logged into.
3. Do not give out the personal contact information of any staff or student unless expressly permitted.
4. Ensure that you act within current legislation relating to the use of IT systems:
    - Data Protection Act 1984 &1998
    - Computer Misuse Act 1990
    - Copyright, designs and patents act 1988

   Breaches of this legislation may result in disciplinary, civil and or criminal action.
5. Always respect the privacy of other users. Do not enter the file areas of other staff without permission.
6. The Network Manager has the right to view any material held in your user area or e-mail.
7. Be Polite and appreciate that other users may have different views to your own. Use of strong language, swearing or aggressive behavior is not allowed.
8. Don't copy work off the Internet or from other staff and try to distribute it as your own. Do not state anything that could be interpreted as Libel.
9. Be sure that any information on the IT Network is accurate and confidential (using password protection where necessary. Make sure you follow the Data Protection Act.
10. You must ensure that you receive appropriate training and documentation in order to use the IT Systems correctly and take steps to ensure this knowledge is kept up to date.
11. Any IT equipment leaving the College must be signed out via the Business manager prior to it leaving College grounds.
12. Any external IT equipment brought into College must first be tested for electrical safety by a member of the IT technical team.
13. You must take reasonable steps to ensure that data introduced into the network externally e.g. via USB drives, optical media and emails are free from viruses and other malware. Any suspected infections must be reported immediately to the IT Support Dept.
14. All software must be used strictly in compliance with the terms of its license and may only be copied if approved by the Network Manager. Under no circumstances must software be placed on the network without the Network Manager's approval.
15. Always lock any computer you are logged into if you have to leave it for a short time. Do not leave computers locked for a protracted period. If a station is found locked for a long time it will be logged off, unsaved work will be lost.
16. You must not exceed or attempt to exceed any access rights to systems or limitations on the use of data granted to you.
17. Due regard must be given to the sensitivity of information when displaying and disposing of information e.g. CDs, USB pen drives, printouts.
18. Take care not to display sensitive information on computer screens or via external devices e.g. multimedia projectors.

19. Be vigilant for suspicious events relating to IT use and report any suspected or actual breach of IT security or vandalism to the IT manager, Network Manager, or in exceptional circumstances the Principal.
20. You have responsibility for backing up data stored off the network e.g. staff portable devices, optical disks, USB pen drives, external hard disks.
21. You must ensure that any private social networking sites or blogs etc that you create or actively contribute to are not confused with your professional role and that you do not accept friend requests from students.
22. You must not engage in any online activity that may compromise your professional responsibilities.
23. Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
24. Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

When using Academy owned ICT equipment remote from the Academy buildings (for example at home)

1. I must ensure that I follow all of the protocols outlined above.
2. When working with sensitive data, especially personal data where an individual is named, I will either use the secure athome service if available, or work from the encrypted memory stick provided by the Academy for this purpose.
3. I must ensure that any sensitive data is encrypted especially personal data where an individual is named. I have an encrypted memory stick provided by the Academy for this purpose.
4. I must only use the device for work purposes.
5. I must allow the anti-virus software to update and scan as set up by the ICT support team.
6. I must return the device to the ICT support team at least once per year when requested so that formal checks on my use of the device and updates to its software can be carried out.
7. No one else must use the device (including family members).

Anyone found in breach of the acceptable use policy may be subject to College disciplinary procedures.

ICT Security Policy - Summary

The objectives of the Policy, which is intended for all College staff, including directors , who use or support the College's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of College information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understands the need for information and ICT security and their own responsibilities in this respect.

The integrity of the Staffordshire Colleges' network depends on the security policy implemented by each connected College.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The College's Network Manager is responsible for the College's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Network Manager will be the official point of contact for ICT or information security issues.

Responsibilities:

Users of the College's ICT systems and data must comply with the requirements of the ICT Security Policy

Users are responsible for notifying the Network Manager of any suspected or actual breach of ICT security. In the absence of the Network Manager, users should report any such breach directly to the Principal, Chair of Governors or to the Council's ICT Unit.

Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.

Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Physical Security:

As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

Server rooms must be kept locked when unattended.

Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

All College owned ICT equipment and software should be recorded and an inventory maintained.

Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.

Equipment should be sited to avoid environmental damage.

- × Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- × Do not give out sensitive information unless the recipient is authorised to receive it.

- Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.

Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security:

- Users must not make, distribute or use unlicensed software or data.
- Users must not make or send threatening, offensive or harassing messages.
- Users must not create, possess or distribute obscene material.

Users must ensure they have authorisation for private use of the College's computer facilities.

The Network Manager will determine the level of password control.

Passwords should be memorised. If passwords must be written down they should be kept in a secure location.

- Passwords should not be revealed to unauthorised persons.
- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data

Passwords should be changed at least every term.

Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.

Regular backups of data, in accordance with the recommended backup strategy, must be maintained.

Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.

Security copies should be clearly marked and stored in a fireproof location and/or off site.

All personal data taken off site must be encrypted.

Virus Protection:

The Network Manager will ensure current and up to date anti-virus software is applied to all College ICT systems.

Portable device users must ensure they update their virus protection at least weekly.

The Network Manager will ensure operating systems are updated with critical security patches as soon as these are available.

The Network Manager will ensure users of home/College portable devices check for critical security patches/Antivirus updates when connecting portable devices to the College network.

Any suspected or actual virus infection must be reported immediately to the Network Manager.

Disposal and Repair of Equipment:

The Network Manager must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.

It is important to ensure that any software remaining on a PC being relinquished is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

The Network Manager must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed

The College will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as College staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Network Manager, or Principal in their absence.

Painsley Catholic College

Consent Form for Staff

Responsible Use of the College Computer Network and Internet Facilities

Please complete, sign and return to IT Support

Name:	***Job Title:***

Staff Declaration

You must read, understand and sign the Acceptable Use Policy if you use our ICT facilities and services. We will keep the completed form in our signed declarations file. You must also be familiar with and understand the implications of the Data Protection guidance, Use of digital and Video Images Policy, the guidance on unsuitable web sites and the policies relating to ICT security, communications, filtering, response to incidents.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users - Staff, and the conditions in the Acceptable use policy. I will use the computer system and Internet in a responsible way and follow these rules at all times when:

- I use the College ICT systems and equipment (both in and out of College)
- I use my own equipment in College e.g. mobile phones, PDAs, cameras etc
- I use my own equipment out of College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College email, VLE, website etc.

Signed:	***Date:***
Please print name:	

APPENDIX B2

Student Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that College ICT systems and users are protected from accidental or deliberate misuse that could put the security of the College and users at risk.

The College will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

Painsley Catholic College

Acceptable Use Policy Agreement

I understand that I must use College ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the College will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. I will inform my parents about the meeting.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the College ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the College ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the College has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the College:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in College if I have permission and certainly not during lessons or educational activities. I understand that, if I do use my own devices in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programs.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of College:

- I understand that the College also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of College and where they involve my membership of the College community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include:
    - A ban, temporary or permanent, on the use of the College computer network / internet facilities. ○
        A letter informing your parents of the nature and breach of rules.
    - Appropriate sanctions and restrictions placed on access to College facilities to be decided by the Head of Year / E-safety Coordinator / Principal.
    - Any other action decided by the Head of Year, E-safety Coordinator, Principal or Chair of Directors of Painsley Catholic College.
    - In the event of illegal activities, the involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to College ICT systems.

If you do not understand any part of this document, you must ask the ICT and E-safety Coordinator, Mr M. Palmer, or a member of the IT Support Department.

Painsley Catholic College

Consent Form for Students

Responsible Use of the College Computer Network and Internet Facilities

Please complete, sign and return to your Form Tutor

Student's name:	***Form:***

Pupil's Agreement

I have read and understand the College Acceptable Use Agreement. I will use the computer system and Internet in a responsible way and obey these rules at all times when:

- I use the College ICT systems and equipment (both in and out of College)
- I use my own equipment in College (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College email, VLE, website etc.

Student Signature:	***Date:***

Parent / Carer's Consent for Internet Access

I have read and understood the College Acceptable Use Agreement and give permission for my son / daughter to access the Internet. I understand that the College will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the College cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the College is not liable for any damages arising from use of the Internet facilities.

Parent Signature:	***Date:***
Please print name:	

Parent / Carer's Consent for Publication of Work and Photographs

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the College website and occasionally in the public media.

The College will comply with the Data Protection Act and request parents / persons with parental responsibility permission before taking images of members of the College. **We will also ensure that when images are published that the young people can not be identified by the use of their names.**

Parents / persons with parental responsibility are requested to sign the permission form below to allow the College to take and use images of their children.

Parent Signature:	***Date:***
Please print name:	

APPENDIX B4

Painsley Catholic College

E- Mail and Internet Use Policy

1 Introduction

1.1 Schools are using E-mail and the Internet more and more to support their activities. This E-mail and Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E-mail and Internet facilities. It applies to all school staff and students who use either or both of these facilities.

1.2 As well as saying what you are not allowed to use E-mail and the Internet for, the policy also provides guidance on the good practices that you should use, and the practices that you should avoid.

1.3 The school will periodically review the policy in response to guidance issued by the County Council.

2 Access to E-mail and Internet services

2.1 Your connection to E-mail or the Internet must be authorised (in writing or in electronic form) by your Network Manager. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Principal.

2.2 The school E-mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable. If you use these facilities, you must keep to and not break any of the conditions in this policy.

2.4 The school has the right to monitor E-mails and Internet use.

2.5 If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

3 Code of Conduct Declaration

3.1 If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration / consent form to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you willfully break the conditions of the policy.

3.2 The school will keep the signed declaration in the IT Office. Sometimes, we may ask you to confirm that you still understand and accept the rules.

4 Specific Conditions of Use

4.1 **General prohibitions**

4.1.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- pornographic or obscene;
- intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our antiharassment and equal opportunities policies in any other way;
- defamatory;
- encouraging violence or strong feelings;
- hateful;
- fraudulent;
- showing or encouraging violence or criminal acts;
- unethical or may give the school a bad name; or
- a deliberate harmful attack on systems we use, own or run.

4.1.2 We will only allow you to do the above if:

- it is part of your job to investigate illegal or unethical activities;
- your Principal or Network Manager asks you to in writing; or
- it is in the public interest.

You must make sure that your Network Manager knows what you are doing. If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your Network Manager who will advise your Principal or Chair of Directors or Internal Audit.

4.1.3 You must not use the school E-mail or Internet facilities for time-wasting activities, such as chain letters, or for sending private E-mails to everyone on the global address list, or for the purpose of bullying or causing or inciting others to cause mental or physical discomfort to any individual.

4.2 **Computer viruses**

4.2.1 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:

- intentionally accessing or transmitting computer viruses or other damaging software; or
- intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

4.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not E-mail material that has not been scanned to other

users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your Network Manager.

4.2.3 You must always follow the instructions that your Network Manager gives you about virus attacks.

4.2.4 If you are not sure how to use the virus protection system, you must get advice from your Network Manager.

4.3 **Passwords**

4.3.1 You must not tell anyone your password, apart from authorised staff.

4.3.2 You must change your password every half term.

4.4 **Other security**

4.4.1 You must not use or try to use the school facilities for:

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- breaking through security controls on any system; or
- accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

4.5 **Publishing information**

4.5.1 You must get authorisation from the Principal for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site. We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

4.6 **Copyright**

4.6.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E-mail or over the Internet.

4.6.2 You must not:

- transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
- knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.

Permission can be sought via e-mail. 4.7

Confidential or sensitive information

4.7.1 You must follow the guidance for the use of personal data as outlined in the College's Personal Data Policy.

4.7.2 You must not break the conditions of the Data Protection Act 1998 when you use the E-mail services of the Internet for transmitting information.

If you need any more advice about these conditions, you should refer to the Policy summary or obtain further information/advice from the Network Manager.

4.7.3 The Internet E-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet E-mail is as insecure as a postcard that you send through the normal post. So, you should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or

legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.4 If you have to transmit any E-mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E-mail.

'This E-mail (including any attachments) is only for the person it is addressed to. If you are not this person, you must delete this E-mail immediately. If you allow anyone to see, copy or distribute the E-mail, or if you do, or don't do something because you have read the E-mail, you may be breaking the law'. This disclaimer can be set using the 'autosignature' facility where this is available.

4.8 **Forums**

4.8.1 There are forums on the Painsley Catholic College website for discussion, social and personal use. These 'bulletin boards' are moderated to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2 Neither the school, the LEA nor the County Council is responsible for the content of any material included in the bulletin board or for anything users do because of the material.

5 Recording Internet use

5.1 You should be aware that use of Internet facilities is logged.

5.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your Network Manager or Principal. If you do not do this, the school may take action against you.

5.3 You should protect yourself by not allowing unauthorised people to use your Internet Facility.

6 E-mail good practice

6.1 The Acceptable usage policy in the staff handbook contains guidelines that tell you what is and what is not good practice when you use internal or Internet E-mail services.

APPENDIX B6

Information and Communication Technology Acceptable Use of Portable Devices Policy (Staff)

- You must only use the device for work purposes. Staff devices are distributed for staff use only. No students or family members are to be allowed to use a staff device.
- It is your responsibility to ensure that all personal data stored on the portable device is adequately backed up in accordance with the backup guidelines included in your machine.
- If a machine needs to have its software reinstalled, any and all software and data, over and above that on the machine at the time of issue, will be lost.
- Any additional software installed by the user should only be done in compliance with the licensing conditions of that software. It is your responsibility to ensure that the machine remains in a legal state after issue by Painsley Catholic Academy.
- Any hardware installed after issue of the machine by the school will be the responsibility of the user. Ensure only the correct manufacturers' drivers are installed.
- Under no circumstances should any portable device be left unattended in a vehicle or public place.
- Any data stored should be done so in accordance with the Data Protection Act, details of which are stored in the school office.
- You must protect your portable device with a login name and password in order to keep personal data secure. This information must remain secret and not written down and placed in your portable device bag.
- Do not give out the personal information pertaining to any member of staff or student at this school.
- Under no circumstances should you view, upload or download any material that is likely to be unsuitable for children. This applies to any material of a violent, dangerous or sexual content.
- Under no circumstances should you use the portable device to download any software or music illegally either through the use of P2P (peer to peer) clients or bit torrent software.
- It is your responsibility to keep the portable device antivirus definitions up to date. Please refer to the IT Support Team to assistance if needed.
- Do not store any files which are protectively marked on your portable device.
- When working with sensitive data, especially personal data where an individual is named, I will either use the secure at home service if available, or work from the encrypted memory stick provided by the Academy for this purpose.
- You must ensure that any sensitive data is encrypted especially personal data where an individual is named. You have an encrypted memory stick provided by the Academy for this purpose.
- You must return the device to the ICT support team at least once per year when requested so that formal checks on the use of the device and updates to its software can be carried out.

- You must ensure that you follow all of the protocols outlined above.

Name of member of Staff: _____

Signature: _____ Date:_____

APPENDIX C0

Advise on Password Changes for Staff

Sent: 16 July 2007 09:31
To: All Staff
Subject: Memo: Password changes

Dear All,

In accordance with the school's ICT Security Policy, all users are required to change their passwords on a regular basis (at least once per year). To simplify things for everyone, we have decided to implement a single username and password policy for staff, so that from September you will use the same username and password for logging into the network, for using SIMS and PARS, and for using SLN2.net. As staff cannot change their own SIMS passwords, I shall be implementing this password change policy over the summer holidays.

As a result, could staff please get back to me as soon as possible with what they would like their password to be. In accordance with the password policy at the school, passwords must:

1. Be at least 8 characters long 2.
Contain both letters and numbers
3. A mixture of upper and lower case.
4. Not be easily guessed (dictionary words or proper nouns).
5. Be capable of being typed quickly so that it is not easily read by an observer.

I am happy to assign arbitrary passwords to anyone who cannot come up with anything suitable, as I appreciate that this is a busy time and due to unforeseen circumstances this memo has come out later than we had hoped.

Additionally, if anyone requires a change to their usernames (for instance if they are getting married, etc) then please let me know and I will process this at the same time.

Thank you in advance,

Network Manager
Painsley Catholic College
RM Certified Network Manager

Don't print this email unless you have to

APPENDIX D

SUMMARY OF ICT SECURITY POLICY

The objectives of the Policy, which is intended for all College staff, students and directors, who use or support the College's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of College information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff and students understand the need for information and ICT security and their own responsibilities in this respect.

The integrity of the Staffordshire Colleges' network depends on the security policy implemented by each connected College.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The College's ICT Manager is responsible for the College's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Network Manager will be the official point of contact for ICT or information security issues.

Responsibilities:

Users of the College's ICT systems and data must comply with the requirements of the ICT Security Policy

Users are responsible for notifying the Network Manager of any suspected or actual breach of ICT security. In the absence of the Network Manager, users should report any such breach directly to the Principal, ICT Manager, Chair of Directors or to the Council's ICT Unit.

Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.

Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Physical Security:

As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

Server rooms must be kept locked when unattended.

Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

All College owned ICT equipment and software should be recorded and an inventory maintained.

Uninterruptible Power Supply (UPS) units are used for servers and network cabinets.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.

Equipment should be sited to avoid environmental damage.

- Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- Do not give out sensitive information unless the recipient is authorised to receive it.
- Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.

Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security: x Users must not make, distribute or use unlicensed software or data. x Users must not make or send threatening, offensive or harassing messages. x Users must not create, possess or distribute obscene material.

Users must ensure they have authorisation for private use of the College's computer facilities.

The Network Manager will determine the level of password control.

Passwords should be memorised. If passwords must be written down they should be kept in a secure location.

- Passwords should not be revealed to unauthorised persons.
- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.

Passwords should be changed regularly.

Passwords must be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.

Regular backups of data, in accordance with the recommended backup strategy, must be maintained.

Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.

Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

The Network Manager will ensure current and up to date anti-virus software is applied to all College ICT systems.

Portable device users must ensure they update their virus protection at least weekly.

The Network Manager will ensure operating systems are updated with critical security patches as soon as these are available.

The Network Manager will ensure users of home/College portable devices check for critical security patches/Anti-virus updates when connecting portable devices to the College network.

Any suspected or actual virus infection must be reported immediately to the Network Manager.

Disposal and Repair of Equipment:

The Network Manager must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.

It is important to ensure that any software remaining on a PC being relinquished is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

The Network Manager must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

The College will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as College staff in relation to not divulging the data or making any unauthorised use of it.

Security Incidents:

All suspected or actual breaches of the ICT security, including detection of computer viruses, must be reported to the Network Manager, or Principal in their absence, who should report the incident to the Staffordshire ICT Service Desk (01785 278000)