POLICY/PROCEDURE TITLE:	**DATA MANAGEMENT**
ISSUE DATE:	**MAY 2009**
LAST REVIEW DATE:	**JANUARY 2015**
NEXT REVIEW DATE:	**JANUARY 2017**
EQUALITY & DISABILITY IMPACT ASSESSMENT COMPLETED:	**YES**
RISK ASSESSMENT:	• **BREACH OF DATA PROTECTION ACT 1998** • **BREACH OF FREEDOM OF INFORMATION ACT 2000**

CONTENTS **PAGE NUMBER**

1. Introduction

Kendal College needs to keep certain information about its employees, students and other users to allow it to monitor its performance, achievements and operate effectively. It is also necessary to process information so that staff can be recruited and paid, so that courses can be organised and various legal obligations to funding bodies and government complied with.

To comply with legislation, information must be collected and used fairly, stored securely and not disclosed to any person unlawfully. To do this, the College must comply with the principles set out in the Data Protection Act 1998. The College is also committed to meeting its legal requirements under the Freedom of Information Act 2000.

Information that is already in the public domain is exempt from the 1998 Act.

This policy should be read in conjunction with the Freedom of Information Policy and the Document Retention policy.

2. Policy Statement

The College will ensure that all personal data is processed fairly and lawfully.

Any member of staff who considers that this policy has not been followed in respect of personal data about themselves, should raise the matter with the appointed Data Protection Controllers initially. The College has two appointed Data Protection Controllers; the Head of College Information and the Finance and Contracts Manager.

3. Procedure

Data Held and Processed

All staff, students and others are entitled to:

- Know what information the College holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the College is doing to comply with its obligations under the 1998 and 2000 acts

Personal Data:

- Must be fairly and lawfully processed
- Must only be obtained for specified and lawful purposes
- Must be adequate, relevant and not excessive in relation to the purpose for which it is required
- Must be accurate and, where necessary, kept up to date
- Must only be processed and kept for as long as is necessary
- Must be processed in accordance with the data subject's rights under the act
- Must be protected against unlawful processing, accidental loss and destruction or damage

- Must not be transferred to a country or territory outside the EEC, unless adequate levels of protection/freedoms are in place

Data Protection Controller

The College has registered under the Act with the Information Commissioner using the template provided for FE establishments. The College has a designated Data Protection Controller (Director of External Relations & Client Services), who is responsible for the College registration under the Act.

Requests for Information

a) Any student, employee, client or person connected with the College may request details of information which they believe the College holds about them.

b) Any person seeking to request access to recorded information on Kendal College may do so by writing to the Freedom of Information Officer (Clerk to the Corporation).

The College will undertake to provide the requested information within 20 working days. The Freedom of Information Officer may refuse to disclose information where the disclosure is not in the public interest or where it could lead to a breach of the Data Protection Act.

Responsibilities of Staff

a) All staff are responsible for:

- checking that information provided to the College in connection with their employment is accurate and up to date
- informing the College of any changes to information, ie change of address
- informing the College of any errors or changes. The College cannot be held responsible for any errors not reported to a member of staff

b) If and when, as part of their responsibilities, staff collect information about others (ie students, references, details of personal circumstances), they must comply with the procedure on personal data under 3 above.

c) The Data Protection Controllers are responsible for keeping this policy updated and relevant

d) The Data Protection Controllers must ensure that the College complies with the Data Protection Act 1998

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed in any way to any unauthorised third party. It should be noted that any unauthorised disclosure may be treated as a disciplinary matter and may be considered as gross misconduct

Personal information should be kept in a locked cabinet or locked drawer. Computerised information should be password protected and/or kept on a disc which is itself kept securely. Passwords should be changed on at least a quarterly basis.

Use of Portable Devices

a) Individuals who use a laptop, tablet or portable device to record, store, process or transmit College-related data must do all that is reasonable to keep their device, associated media and the data contained therein secure at all times. Due to their portable nature, personal devices should not be left unattended when used off-site or during the course of a journey, nor should they be left exposed on the seat of a car or other vehicle. Access should always be restricted by use of a system password.

b) When processing personal data on laptops or portable devices, all reasonable steps must be taken to ensure the security of that personal data. In particular, personal data must not be processed in public places e.g. when travelling on public transport. All processing should be carried out in privacy to avoid accidental disclosure to non-authorised persons.

c) Individuals who use a small portable device to store College-related data must do all that is reasonable to keep the device and the data contained therein secure at all times.

d) Examples of small portable devices include:

- Palm-held and Pocket computers
- Tablets including College issued i-pads
- PDAs (Personal Digital Assistants)
- Mobile Phones
- USB Data Keys
- Removable Disk Drives
- Iomega Zip, Jaz and PocketZip Disks
- Small memory cards (e.g. Sony MemorySticks, Compact Flash memory, Smart Media cards, MultiMedia cards, Secure Digital memory)
- Tape Media
- Other storage media, including CD-ROMs, DVDs, floppy disks

e) Data must not be carried on small portable devices unless it is adequately secured. Access to the device should be protected by using a password or Personal Identification Number (PIN), if at all possible. Data encryption features should be utilised, where available.

f) Sensitive personal data, as defined in the Act, should not be stored in a portable device unless it can be demonstrated that special security precautions have been taken e.g. encryption of files on the hard disk or on a storage medium.

g) The Data Protection Controller should be contacted immediately in the event of the loss or theft of any portable device.

h) It should be noted that failure to implement appropriate security measures when using portable devices for the storage of personal data may be treated as a disciplinary matter and could be considered as gross misconduct.

References

Staff members who are requested to provide an employment reference in their professional capacity at the College should adhere to the following guidelines:-

- All data provided in a reference should be based on fact or should be capable of independent verification. As a guide, references should be fair, accurate and not give a misleading overall impression of the employee.
- Referees should avoid giving any subjective opinion about an individual's performance, conduct or suitability, unless it can be substantiated with factual evidence.
- The Referee has a duty of care to both the individual about whom it is written and the recipient of the reference, therefore references should be prepared with due care.
- The Personnel Department should be contacted for further advice if there is any doubt or queries in relation to providing a reference.

Conclusion

Compliance with the Data Protection Act 1998 is the responsibility of all members of the College, and staff should be mindful of the following:

- No undue pressure should be placed on anyone to disclose personal data
- No personal data should be disclosed over the telephone unless the caller has been properly identified and is entitled to the data
- Any special request for disclosure of personal data, eg to the Police or Inland Revenue, should be referred to the Data Protection Controllers who will manage and log the request
- Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

4. Linked policies

- Freedom of Information Policy
- Document Retention Policy
- IT User Policy