

Security of Personal Data Policy and Guidelines

Written by Richard Lane, April 2009

Updated for subject access requests February 2011

1 Introduction

KCC holds personal data on staff and students in order to achieve the efficient running of the College. Data is held in computer systems and also in paper record form. Generally, people are entitled to expect their personal information to be kept private. This entitlement is backed up by the Data Protection Act which places legal duties on organisations handling personal data – such as KCC. This document should be read in conjunction with The Acceptable Use of IT Policy and data backup/recovery policies/procedures. Where KCC works in premises controlled by other organisations (for instance prisons), the policies of those other organisations will take precedence over this policy unless it is looser than this policy or the college possesses written agreement to vary that policy.

2 Policy

KCC is fully committed to compliance with the requirements of the Data Protection Act 1998 (“the Act”), which came into force on the 1st March 2000. KCC will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, or partners who have access to any personal data held by or on behalf of KCC, are fully aware of and abide by their duties and responsibilities under the Act.

2.1 The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable. The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

2.2 Types of Personal Data

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data. Personal data is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Bank details are also highly sensitive.

2.3 Handling of personal/sensitive information

KCC will, through appropriate management and the use of strict controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one’s personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, KCC will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All managers and staff within KCC are to be made fully aware of this policy and of their duties and responsibilities under the Act. They will be made fully aware of this policy and take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers, computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or agents of KCC must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of KCC, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between KCC and that individual, company, partner or firm;
- Allow data protection audits by KCC of data held on its behalf (if requested);
- Indemnify KCC against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by KCC will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by KCC.

2.4 Responsibilities

KCC has appointed a data protection lead manager, currently the Director of Resources. This lead manager will be responsible for ensuring that the Policy is implemented. The lead manager will also have overall responsibility for:

- The provision of cascade data protection training, for staff within KCC.
- For the development of best practice guidelines (see attached).
- For carrying out compliance checks to ensure adherence, throughout the College, with the Data Protection Act.
- The lead manager will review and renew KCC's Data Protection Registration annually.

All KCC staff, contractors and partners are expected to comply with this policy insofar as they come into contact with personal data through KCC. Staff or students who consider that the policy has not been followed in respect of personal data should raise the matter with KCC's lead manager in the first instance.

Security of Personal Data Guidelines

1 Status

Compliance with these guidelines – or other local guidelines where stricter - is mandatory for all KCC staff. A copy should be displayed in HR, Payroll, MIS, Admissions, by photocopiers and fax machines.

2 Collection and Recording

In order to ensure the security of personal information,

- Staff working with personal data on a PC should ensure that the screen cannot be seen by someone who should not have access to the data.
- PCs should be set up with a password protected screensaver (right click on the desktop, select properties, screen saver and tick password protect on resume to set this up).
- All forms and questionnaires requiring people to fill in personal information must include a data protection statement which explains who will use the information and for what purpose.
- Website forms inviting people to submit personal information must always comply with appropriate security protocols (SSL).
- CCTV will only be used to monitor external doors, entrance lobbies and locations where there is a high risk of break-in or theft.

3 Transmission and Carriage

It is not normally appropriate to include personal information or an opinion about someone in an email. Extreme care should be exercised when transmitting/sending files containing personal data about more than one person through the internet, by post or some other means. Only the following methods of transmission/carriage are permitted:

- A file can be uploaded to a secure channel (such as the LSC's data portal).
- A file can be converted into an encrypted zip file. Small files of less than 100 records can then be emailed. Larger files or files containing sensitive information should then be written to a CD and sent by courier. The password for encrypted files should be telephoned through - not put on an email.
- All sent/transmitted files should be stripped of all unnecessary information. For example, a surname may not be required if the learner reference number is included.
- Transmission of personal data from one KCC Groupwise email account to another KCC Groupwise email account, provided the data is needed by the recipient for a legitimate purpose, is secure and acceptable.

It is not permitted to send printouts of databases of personal records through the post or by courier.

It is not permitted for prisoners' names to be included in any information sent out of prison Education Departments. Prisoners should be identified by prison number only.

Personal information for up to 10 people may be conveyed by phone or faxed, although care should be taken to ensure that sensitive information is not left on a fax machine or in a tray which is accessible to people who should not see it.

Forms for up to 10 individuals can be posted using recorded delivery. Forms for more than 10 people should be hand delivered or conveyed by courier. The sender of the information is responsible for ensuring that it has been received by the receiver. Forms sent by internal post must be put in an envelope. Post rooms must be kept inaccessible to casual passers by.

4 Disclosure

Personal details may only be disclosed to third parties in the following circumstances:

- On receipt of written instructions from the subject of the personal information.
- Student records can only be disclosed by the MIS Manager.
- Staff records can only be disclosed by the HR Manager or Finance Manager (payroll information).
- All disclosures must be logged with the Director of Resources and the authority letter filed with and cross-referenced to the log.

5 Storage, Retention and Disposal

Personal information in paper form should only be held in approved, secure locations. These locations must be locked to a standard approved by insurers and the files held in a locked cupboard, when not in use. One locked door is sufficient for files held in an archive cupboard which is only occasionally accessed.

- Personal information about members of staff in paper form is only allowed to be held within the HR or Payroll offices or their archives. Managers should not hold their own records on staff except the minimum of day-to-day records which should be held for no more than 1 year.
- Personal information about students in paper form is only allowed to be held within the MIS office, Reception offices, prison admin. offices or their archives. Academic department staff may hold the minimum of day-to-day records about students. These records should be held for no longer than 1 year or the length of the course, if longer. Information about no more than 20 students is only allowed to be taken off-site for day-to-day processing (such as marking or assessing). Storage of personal information about students off-site is not permitted.

Paper documents showing personal information should never be left out in view of cleaners or other visitors to offices. Cleaning staff are only permitted in offices containing large amounts of personal information (HR, Payroll and MIS) when a member of staff is also present.

Staff are not permitted to store personal data in electronic form on any media other than in authorised installations such as the College's MIS system, HR system,

payroll system or network filing system. Personal data must not be stored on a PC's C drive or My Documents folder. Neither should it be stored on floppy disks, CDs, memory sticks, laptops or other portable memory devices. The minimum of contact details for no more than 50 individuals may be stored on mobile phones.

CCTV recordings are held in a secure location for no longer than 1 year.

Information about students should not normally be retained for more than 6 years after the last contact/transaction. Records relating to ESF funded projects may be kept longer, according to the requirements of the project. The College is required to hold some information about staff in perpetuity. Paper records of personal data which are no longer needed must be shredded. It is not permitted for these records to be put in waste bins without being shredded.

6 Breaches and Queries

All breaches of this policy and guidelines must be reported using the accident/incident reporting system. Queries relating to these guidelines should be addressed to the Director of Resources.