

EMMANUEL COLLEGE

THE APPLICATION OF THE DATA PROTECTION ACT 1998

Contents

1. Introduction	Page 2
2. The Data Protection Act 1998	Page 2
3. Review of data used in College departments	Page 3
4. Security	Page 4
5. Staff code of practice for data processing	Page 5
6. Employee records	Page 5
7. References	Page 5
8. Disclosure of information to third parties	Page 6
9. Subject access requests	Page 7
10. CCTV	Page 7
11. College web site	Page 7
<u>Appendix A:</u> Emmanuel College policy for the processing of personal data	Page 8
<u>Appendix B:</u> Examples of the classes of personal data processed by the College	Page 9
<u>Appendix C:</u> Examples of the categories of data subjects on which data may be held	Page 10
<u>Appendix D:</u> Staff code of practice for data processing	Page 11
<u>Appendix E:</u> Guidance notes for the preparation of references	Page 13
<u>Appendix F:</u> Operational procedures for Emmanuel college CCTV system	Page 15

THE APPLICATION OF THE DATA PROTECTION ACT 1998

1. Introduction:

The policy set out below has been adopted in order to ensure that all data identifiable as relating to a living person, which is held by the College or used by it, is handled in a fair, accurate and secure manner that is consistent with the Data Protection Act 1998.

2. The Data Protection Act 1998:

For the purposes of the Data Protection Act 1998 the following arrangements apply to the College:

All data which the College holds about a living person, who can be identified from the data, or identified from the data in conjunction with other information, is defined as **Personal Data** and is subject to the provisions of the Data Protection Act 1998. The Act covers Personal Data held not only in electronic records but also in structured 'manual' (i.e. paper) records.

Sensitive Personal Data, relates to racial or ethnic origin, political opinions, religious or other similar beliefs, state of health, 'sexual life', membership of a trade union, or (alleged) commission of any offence.

Data Subjects are the individuals relating to whom the College holds or uses Personal Data. The Data Subjects are students, Fellows, staff, applicants, and others such as suppliers, alumni and members and supporters of the College.

The College has notified the Information Commissioner as to the **purposes** for which it holds and processes Personal Data. A copy of the College notification can be seen at: <http://www.dpr.gov.uk/search.html> or a copy can be obtained from the Bursar.

In broad terms, the **purposes** for which the College processes data are: student and staff support services, research functions, alumni relations, education and training administration. Data may only legitimately be processed for the purposes stated, and not for other purposes of which the data subject has not been informed.

The **Data Controller** for the College is the Bursar. All questions concerning the processing and disclosure of personal data should be referred to the Bursar.

Under the terms of the Data Protection Act 1998:

The College may process Personal Data if:

1. The processing is necessary for the purposes or legitimate interests pursued by the College; **or**
2. The data subject has given their consent to the processing of the data.

When data processing is necessary for the purposes or legitimate interests pursued by the College, and processing does not prejudice the rights, freedoms and legitimate interests of the data subject, there is no need for the consent of the data subject to be obtained.

However, all processing of Sensitive Personal Data requires the explicit consent of the Data Subject. **Sensitive Personal Data cannot be held or processed without the explicit consent of the Data Subject.**

All processing of Personal Data by the College must abide by the principles set out in the Data Protection Act 1998. These principles are that data must be:

1. processed fairly and lawfully
2. obtained for specified and lawful purposes
3. adequate relevant and not excessive
4. accurate and where necessary kept up to date
5. not kept for longer than necessary
6. processed in accordance with the subject's rights
7. kept secure
8. not transferred abroad without adequate protection

The College must inform all of those for whom the College holds Personal Data of the categories of data which are held and the purposes for which data is held. For example, students will be informed of the data which the College holds and processes at the time of matriculation, and they will sign the following statement:

'I consent to the processing by the College and the University of personal data, including sensitive personal data as defined in the Data Protection Act 1998, about me for the proper purposes of these institutions. I undertake to observe the provisions of the Data Protection Act 1998 in relation to any personal data I may myself hold and process as a student of the College and the University, and I agree to indemnify the College and the University from liability for any claims or damages that may arise from the processing of this data'.

The Emmanuel College policy for the processing of Personal Data, which is available for circulation to students, staff and others, is set out at Appendix A.

3. Review of data used in College departments:

Data requirements and the purposes for which data is held vary between College departments.

In order to ensure that data is held and used in a fair, accurate, and secure manner it is necessary for each relevant department to draw up a statement detailing the arrangements which will apply in that department. The policy statement should be produced by the Head of Department, in consultation with the relevant College Officer, and should cover the following:

1. What broad classes of Personal Data are held or processed in the department and for what purpose. Examples of data classes are set out at Appendix B.
2. For which categories of Data Subjects is Personal Data held. By what means is each category of Data Subject informed of the purposes for which the College holds and processes Personal Data. Examples of Data Subject categories are set out at Appendix C.
3. Which members of staff within the department have access to each category of Personal Data.
4. Is any of the information held or processed in the department defined as Sensitive Personal Data. The definition of Sensitive Personal Data is set out in section 2 above. If so is explicit consent for processing obtained?

5. Are any department-specific variations upon the College's general security provisions (set out at 4 below) necessitated by the physical layout of the department, the nature of the computer hardware or software employed, or arrangements for visitors to the department etc?
6. What is the policy operating within the department relating to the retention and deletion of Personal Data? The policy should ensure that no data is held longer than necessary, and that when it is retained there is a sound reason for its retention. It should state the arrangements for reviewing data at certain significant dates (for example, graduation or the completion of the admissions round), and the policy for weeding or destroying data at that point. The policy should also detail arrangements for transferring data to the archives or other secure storage as necessary. The policy may, as appropriate, specify arrangements for the periodic review of data so as to ensure, in so far as is possible, that it remains accurate and relevant, in the knowledge that the data might at some point be shown to the individual to whom it relates.

4. Security:

The College must ensure that all reasonable steps are taken to ensure that personal data is stored and processed securely.

The following precautions will be taken:

Access to computer files containing Personal Data must be restricted using privilege levels and passwords.

Regular password changes will be enforced and the number of attempted logins limited.

Computer equipment must be sited in a secure location where access can be restricted to authorised personnel only.

Computer screens must be sited so that they cannot be viewed by members of the public.

Computer terminals should not be left unattended and should be logged-off at the end of a session; remember:

'log-off, switch-off, lock-up'

Redundant data must be regularly wiped or over written in accordance with the policy applying in each College department.

Data must be backed up stored securely. Back-up tapes should be stored at a separate location.

Floppy disks must be locked away after use.

Where computer systems containing personal data are connected to an external network, a recognised firewall will be installed.

Computer printout containing personal information must be shredded before disposal; it must not be used as scrap paper.

All manual Files must be stored securely. It is the responsibility of each Head of Department to ensure that appropriate secure storage arrangements operate in each department.

5. Staff code of practice for data processing:

A copy of the College's code of practice for data processing carried out by members of staff is attached at Appendix D.

6. Employee Records:

All information in a personnel file should be considered to be Personal Data and must be processed in accordance with the principles set out at 2 above.

It is necessary to hold Personal Data on employees for the effective administration of their employment and for the purposes and legitimate interests pursued by the College. However, at the time that employment begins, employees need to be informed of:

1. The broad categories of Personal Data which the College holds and processes,
2. The broad purposes for which the College holds or processes Personal Data about them,
3. The identity of the College's Data Controller,
4. The College's Data Protection policy statement (attached at Appendix A).

Job application forms need to explain the purpose for which information will be used by the College, and also need to state that the information provided will not be used for any purpose other than considering the application.

Sensitive Personal Data must not be held on an employees file without the **explicit consent** of the employee. The only exception to this is if Sensitive Personal Data is held in order to comply with a legal obligation applying to the College, for example, under health and safety legislation or to comply with the Disability Discrimination Act. Sensitive Personal Data must only be retained for as long as it necessary or for the purposes of defending a complaint of unlawful discrimination or as means for monitoring, promoting, or maintaining an Equal Opportunities Policy.

It is legitimate to retain copies of spent warnings, as the retention of the disciplinary record may be essential in determining an employee's suitability for development and promotion etc.

Health and sickness information must not be disclosed without **explicit consent** (e.g. in references).

7. References:

References received:

Confidential references received by the College and placed in a relevant filing system are Personal Data. Referees should be requested to indicate in writing whether or not they consent to their reference being disclosed to the Data Subject in the event of an access request being made by the Data Subject. Requests for references should explain this procedure and provide an easy method for referees to indicate whether or not they consent to disclosure. No response to such a request should be taken as consent to disclosure (and this should be explained to the referee). References cannot be released to Data Subjects if the referee has refused consent.

References provided:

The College is not required to disclose references it provides, however, these references may be disclosed by those receiving them. References should therefore always be written on the basis that they may be seen by the Data Subject, but when providing a reference the referee should state whether or not they consent to disclosure. One way of avoiding problems is if referees send a copy of the reference to the Data Subject at the time that it is written. While the College is not required to disclose references it has written, these references must still be fair, accurate, relevant, and demonstrably

factual, and the views expressed in them must be justifiable by the author from his or her first hand knowledge. Guidance notes for the preparation of references are attached at Appendix E.

8. Disclosure of Information to Third Parties:

Personal Data must not be disclosed to third parties without the Data Subject's consent.

If the College is approached by a third party requesting information about a student, Fellow, or other person about whom the College may hold Personal Data, information must not be disclosed without that person's consent. This may apply even when an inquiry is made by a member of the person's family, their friends, local authorities, government bodies, and the police, and applies even when the request is for basic information such as their address or telephone number in College. However, there are circumstances in which the College has a statutory duty to disclose information to public bodies, for example the Benefits Agency.

The following are examples of ways in which requests for information from third parties should be handled:

1. If a telephone caller or visitor is trying to contact a student, the student's room number, address or telephone number should not be disclosed. An offer to pass a message to the student informing them of the inquiry is the appropriate response.
2. If a request for an e-mail address for an individual is received, the enquirer should first be referred to the e mail search facility on the University web site, if the person cannot be identified there, it is appropriate to respond that:

‘The person that you are looking for is not in the world readable e-mail directory and we cannot provide any further information. If we are able to contact the person we will forward a message for you if you wish us to do so.’
3. A personal e mail address should only be provided following an enquiry relating to a member of staff if that address is already the published contact.
4. Unless the consent of the Data Subject has been obtained, the following categories of information should not be released to a third party:
 - Confirmation of degrees and examination results
 - Confirmation of residence from banks, Councils etc
 - Transcripts and degree certificates
 - Police inquiries
 - Electoral roll inquiries
 - Requests for data from other students

In other situations in which a request for information is made, and the inquirer has not been able to obtain the consent of the Data Subject, or that consent has been withheld, the matter must be referred to the Data Controller (ie the Bursar). This is the case even when the inquiry comes from a public body such as a Council or the Police. Requests must be passed to the Data Controller quickly so as to ensure a response within the time limits laid down by the Data Protection Act.

The only occasion when Personal Data may be disclosed without the Data Subjects consent is if disclosure protects the subject's health and safety or it is in other ways required by law. Where the Data Subject's consent is not available, the Data Controller must be consulted before any disclosure is made.

The College will ensure that all Personal Data is kept secure from unauthorised use and disclosure (see 4 above concerning security).

9. Subject Access Request:

Fellows, students and members of staff regularly ask the College to provide information about them, for example a reference or an exam transcript. Such requests are unaffected by the Data Protection Act and, at the request of the Data Subject, this information should continue to be provided in the normal way.

However, if the College is asked by an individual to provide a copy of data which the College holds about them, this is a **Subject Access Request**.

All Subject Access Requests must be referred to the Data Controller, i.e. the Bursar.

Examples of Subject Data Requests are:

- A member of staff might request access to information from their personnel record
- A student might request access to information held on their Tutorial File
- An applicant might request to see a copy of their interview report

In each case the request must be referred to the Bursar as Data Controller.

A Subject Access Request must be made in writing to the Bursar as Data Controller.

When a Subject Access Request is received the Bursar will:

- if necessary, clarify the nature of the request so as to enable the data sought to be located,
- confer with the relevant Heads of Department to clarify the data which is held,
- respond to the request within 40 days, confirming the data held, the source from which it was obtained, the purposes for which it is held, to whom it may be disclosed, and providing a hard copy of the data requested.
- charge the Data Subject a fee of £10.
- in responding to the Subject Access Request, the Bursar will exclude information which, by supplying it, would breach the confidentiality of a third party would.

10. CCTV:

A copy of the College's policy relating to the use of CCTV cameras and recording equipment on the College site is attached at appendix F.

11. College Web Site:

Each College Department (the Tutorial Office, the Development Office, Information Systems) which enters content onto the College web site must ensure that consent has been obtained from any individual whose details, for example e mail address, are to be included, unless those details are already available from some alternative publicly accessible source. An exception to this is contact details in the College (i.e. phone number and e mail address) for members of staff who are identified according to their job title.

APPENDIX A

Emmanuel College Policy For the Processing Of Personal Data

The Data protection Act 1998 sets out rules for processing personal information, and these apply to some paper records as well as those held on computer. The Act gives individuals certain rights, and also imposes obligations on those who record and use personal information to be open about how information is used and to follow eight data protection principles.

Personal data must be processed following these principles so that data are:

1. processed fairly and lawfully
2. obtained for specified and lawful purposes
3. adequate relevant and not excessive
4. accurate and where necessary kept up to date
5. not kept for longer than necessary
6. processed in accordance with the subject's rights
7. kept secure
8. not transferred abroad without adequate protection

Your rights:

You are entitled to have access to information held about you, except where releasing that information would breach another person's privacy. You also have rights to prevent data processing likely to cause unwarranted damage or distress, and to prevent processing for the purpose of direct marketing.

Your responsibilities:

Any personal data which you yourself hold must be collected, processed and held according to the data protection principles set out above. If you possess data on your own behalf, you are responsible for compliance with the law. The College is responsible for data collected for its own proper purposes, and if you have access to this data you must follow the relevant policy and procedure specified by the College.

How your data is used by the College:

Information is shared between the College and the University, and is used for a full range of student administration including education, research, support services, statutory returns, alumni relations, accounts, public relations, security and crime prevention. Information is supplied regularly by the College to the University Students Record Office, the University Careers Service, the University Registry, the University Disability Resource Centre and University Development Office.

Full details of the College's notifications with the Information Commissioner are available at:

<http://www.dpr.gov.uk/search.html>

A copy of the College notification may also be obtained on request from the Bursar.

If you have any queries about how your data are used, or the application of the Data Protection Act, please contact the College Data Controller, who is the Bursar.

APPENDIX B

EXAMPLES OF THE CLASSES OF PERSONAL DATA PROCESSED BY THE COLLEGE

The following is a list of standard descriptions of data classes. Data classes are the types of personal data which may be processed by College departments.

- **Personal details**

Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addressees, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, eg NI number.

- **Family, lifestyle and social circumstances**

Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

- **Education and training details**

Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

- **Employment details**

Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and terminations details, attendance record, health and safety records, performance appraisals, training records, security records.

- **Financial details**

Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.

- **Goods or services provided**

Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

The examples given above are not an exhaustive list of what may be included in each category.

The following categories of data have been designated as sensitive personal data.

- **Racial or ethnic origin**
- **Political opinions**
- **Religious or other beliefs of a similar nature**
- **Trade union membership**
- **Physical or mental health or condition**
- **Sexual life**
- **Offences (including alleged offences)**
- **Criminal proceedings, outcomes and sentences**

APPENDIX C

EXAMPLES OF THE CATEGORIES OF DATA SUBJECTS ON WHICH THE COLEGE MAY HOLD PERSONAL DATA.

The following is a list of standard descriptions of data subjects. A data subject is an individual about whom personal data are held.

- **Staff including volunteers, agents, temporary and casual workers**
- **Customers and clients**
- **Suppliers**
- **Members or supporters**
- **Complainants, correspondents and enquirers**
- **Relatives, guardians and associates of the data subject**
- **Advisers, consultants and other professional experts**
- **Patients**
- **Students and pupils**
- **Offenders and suspected offenders**

All of the above categories include current, past or prospective data subjects

APPENDIX D

EMMANUEL COLLEGE

STAFF CODE OF PRACTICE FOR DATA PROCESSING

The College recognises that all staff must have access to appropriate information in order to fulfil their job responsibilities. At the same time, data relating to students, Fellows, staff or others must be processed fairly and lawfully, and in a manner consistent with the principles established by the Data Protection Act 1998. Those principles state that data must be:

- processed fairly and lawfully
-
- obtained for specified and lawful purposes
-
- adequate relevant and not excessive
-
- accurate and where necessary kept up to date
-
- not kept for longer than necessary
-
- processed in accordance with the subject's rights
-
- kept secure
-
- not transferred abroad without adequate protection

These principles apply to the storage or use of all information about a living person, who can be identified from the data, or identified from the data in conjunction with other information. In order to avoid confusion, it should be assumed that these principles apply to all data stored or processed by the College.

In order to comply with these principles, the following arrangements must be observed.

1. You must obtain authorisation from your Head of Department before accessing or using administrative information.
2. You must clearly label confidential information and ensure that such information is kept securely.
3. When an office is left unoccupied it must be locked securely.
4. Any password issued to you which gives you access to the College computer systems must be kept securely and kept to yourself, i.e. not passed on to a third party.
5. Any anti-virus arrangements or the use of anti-virus software, which is notified to you periodically by the College must be applied to check all diskettes imported into the College computer systems.
6. You must ensure that arrangements for making backup copies of important data are observed and that any copies are stored securely
7. You must ensure that any stored information is removed before disposing of old equipment or media

8. You must obtain authorisation before taking data or equipment out of the office in which you work.
9. You should be aware that electronic mail is not a secure medium, and you must observe the College's e-mail and internet policy.
10. You must not install or use any untested software without authorisation from your Head of department..
11. You should be aware that the standard encryption for Word Processors is not secure and must not be relied upon.

October 2001

APPENDIX E

REFERENCES

In a recent decision, the House of Lords ruled that the author of a reference owes a duty of care to the person about whom it is written, and may be liable in damages to that person if loss is caused through negligence. Hitherto it had been thought that there would be liability only in defamation, and then only if it could be proved that the writer was motivated by malice. Liability may now come about through carelessness either as to matters of fact or in the formulation of opinion. The author of a reference has therefore an obligation to the subject of the reference. The House of Lords did not consider whether the author also has an obligation to the recipient of the reference, although such a liability is likely.

The College has insurance that covers both itself and individual members of staff (as employees of the College) against claims arising from a reference. This covers references written by a member of staff in the context of his/her employment in the College – ie, references on behalf of students, fellow academics, other members of staff, etc. It does not cover references where the individual is acting in his/her private capacity (eg, a character reference on behalf of a friend or neighbour).

There are two principal aims of a reference:

- To confirm facts – to confirm the accuracy of the statements made in an application: the claim of “experience of Admissions work” may be based on three weeks making up enrolments packs as a summer job;
- To provide opinions – to give the referee’s opinion as to the candidate’s suitability for the post/course in question, and his/her potential for the future.

The reference relies on both facts and opinions, and these two should be clearly differentiated.

The following recommended guidelines relate specifically to student references, but the principles are equally applicable to all references:

- If you are likely to be asked to give a reference, prepare in advance, you will normally be asked to act as a referee by a student and it is therefore sensible to collect relevant information to make the composition of the reference a relatively easy task. Remember the provisions of the Data Protection Act: a student has the right to have a printout of any material held on computer.
- Try to be fair to both the student and the recipient of the reference.
 - **Ensure that the reference is factually accurate and complete**
- Make sure that your opinions are clearly stated as opinions, are based on fact, and that you are qualified to give such opinions:

Do not confuse fact and opinion: “on her performance to date, I would be surprised if X did not get a first class degree” is clearly an opinion; “she will get a first class degree” suggests that the method of classification for Honours is such that the issue is beyond doubt.

Ensure that the opinions you state are honest opinions based on facts known to you. Do not make statements which you are not qualified to make. For example, “I consider X to be well suited to the post for which s/he has applied, and am happy to support his/her application” is better than “X will be a success in the post of....”

For this reason, particular care should be taken where you are asked for a reference for a student who is not known to you. Do not give an opinion which is not your own, just because the person who knew the student has left. It is preferable to quote someone who has knowledge of the candidate, giving the source of the quote.

There may be issues on which you are asked to express an opinion on which you have limited knowledge – eg honesty and integrity. Here you may have to say, for example, “...I know nothing that would lead me to question X’s honesty...”

- Avoid using ambiguous or ‘coded’ language – for example, “X has studied here for three years, during which time he has done his work entirely to his own satisfaction”.

Telephone references: The same guidelines apply to references given over the telephone: do not be tempted to make incautious statements simply because they are not in writing. Ideally, references should not be given over the telephone (you do not know how the information will be filtered as it passes through the various stages of what the enquirer understood you to say; what s/he jotted down; what s/he orally reported to the panel). However, requests for telephone references appear to be increasing. You should resist such requests other than in exceptional circumstances, when you should limit the information to facts and follow up immediately with a Fax.

A copy of any reference you give should be placed on the relevant student file.

If you are challenged over a reference you have given, refer the matter to the Senior Tutor or Bursar as soon as possible.

APPENDIX F

Operational Procedures for Emmanuel College CCTV System

There is a close circuit television system (CCTV) in use in Emmanuel College, the cameras installed transmit their pictures to the Porters Lodge where they can be viewed on a 'real time' basis and are also recorded on a video system for archive purposes, and for replay in the event of an incident.

The object of the system is: -

1. To create a safer working environment for staff and students in the college
2. To protect property, belonging to the College, Student and Staff.

The CCTV system will be used solely for the purpose of security surveillance and, when necessary, the provision of evidence in support of any enquiry or prosecution that is associated with criminal activity committed on College property, or the misuse of College rooms or equipment.

Cameras should not be used to infringe an individual's right to privacy.

Operation of the CCTV controls is restricted to members of the Porters Lodge, or other persons authorised by the Bursar.

Video Tape Procedures

The following procedures, concerning the use and retention of videotapes, are to be followed in order to provide an acceptable level of security and accountability, and to ensure the acceptance of videotape recordings in support of criminal proceedings.

Details are to be recorded in a CCTV Logbook maintained in the porters lodge on a daily basis.

- a. Videotapes are to be changed once a day at midnight.
- b. An entry is to be made in the CCTV register giving the reference number of the tape put into the machine together with the time, date and identity of the porter changing same.
- c. A similar entry will be made in the register to cover the removal of the tape for the previous day.
- d. In the event of a tape being taken out of the machine for any reason throughout the day, the next available tape will be put in the machine, and an entry will be made in the relevant sections of the register.
- e. The recorded tape will be stored in a tape storage unit, and will be retained for 14 days, after which it will be erased and can then be re-used. An entry will be made in the logbook when it is erased.
- f. If an incident occurs and it is thought that the CCTV system has some evidence on it, then the tape concerned should be removed and placed in a signed, sealed envelope, together with a note saying what the incident was, an approximate time, which camera to view and the name of the porter removing the videotape from the system, This should be handed to the Head Porter as soon as possible.**

Viewing Tapes

The Bursar, Head Porter, or a person nominated by them, may view tapes. If a tape is viewed a record has to be kept as to who viewed it, when and for what reason.

Any recorded tape that is requested by the Police in connection with a criminal enquiry will be released to them against the officer's signature in the tape register.

If we are asked to retain a tape for evidential purposes, in connection with a criminal activity, the Head Porter will take possession of the tape for as long as is required, which is usually until one month after the finalization of any court proceedings.

Any request by third party to view a CCTV recording **has to be approved** by the Bursar.

On no account will CCTV video recordings be viewed by any unauthorised person, or removed from the Porters Lodge without the specific approval of the Bursar or Head Porter.

Staff are informed that misuse or unauthorised use of the CCTV system will be considered as a serious discipline matter.

Additional information

The Head Porter, or a nominated deputy is responsible for ensuring that the CCTV equipment is maintained in a suitable condition.

The Head Porter, or a nominated deputy is responsible for ensuring that all new tapes are given a unique reference number, and for replacing old tapes once they have been re-used 12 times.

The Head Porter, or a nominated deputy is responsible for erasing the tapes contents after the 14-day period, and making the relevant entry in the CCTV register.

The Head Porter, or a nominated deputy is responsible for ensuring that the CCTV logbook is kept in a suitable manner. Old logbooks should be kept for a period of one year.

