Northampton College

POLICY STATEMENT

TITLE:	**Data Protection and Privacy Policy**
INTRODUCTION/OVERVIEW:	This policy sets out the College's approach to the way it stores, handles and allows access to information about its employees and students.
POLICY STATEMENT:	The College recognises that it has a duty to secure any information it holds and to only hold information which it reasonably needs to discharge its function as an employer effectively. This policy (and annexes) sets out the way that information will be protected and handled by employees and students.
QUALITY STATEMENTS:	• The College will adhere to the key principles relating to the use of data as defined in the Data Protection act 1998. • The College will ensure that the interests of its employees and students are safeguarded by regularly reviewing its policy and by taking account of the Code of Practice and other advice provided by regulatory authorities. • The College will appoint a designated Data Protection Officer who will complete the annual registration for the Information Commissioner
LINKED POLICIES/ PROCEDURES:	• Staff Disciplinary Policy • Student Disciplinary Policy • ICT Security Policy • ICT Acceptable Use Policies • CCTV Policy • Safeguarding Children and Vulnerable Adults Policy • "Working with Students" guidelines • Staff References guidelines • Staff Recruitment Policy
MONITORING PROCEDURE:	Annual HR file audit Internal/External Auditor Report
DATE FOR REVIEW AND NEXT DIVERSITY IMPACT ASSESSMENT:	This policy will be reviewed and revised periodically, particularly in the light of any developments in employment legislation or good employment practice, in order to ensure its continuing relevance and effectiveness.
RESPONSIBILITY: **Overall (Directorate/Dept):** **Implementation:**	Information & Student Services/Human Resources Head of Information Services/Director of Human Resources

APPROVED BY SMT: (Principal to sign)	**(Signature)**
	Principal **(Position)**
	(Date)

OR

ENDORSED BY SMT AND APPROVED BY CORPORATION: (Principal to sign)	**(Signature)**
	Principal **(Position)**
	(Date)

Contents

1. INTRODUCTION

Northampton College needs to keep certain information (computer or paper based) about its employees, students and other users to allow it to monitor such areas as performance, achievements and health and safety. It is also necessary to process the information so that the College meets all legal obligations to our funding bodies and government agencies.

This policy highlights the key issues relating to data protection and Northampton College. It is intended to provide guidance for College employees, all of whom have an important role in ensuring the legislation is adhered to.

All employees and students must comply with the College policies and procedures relating to data protection. In depth guidance for employees and students can be found in appendix 3, 4 and 5.

This policy aims to ensure that the College complies with its legal requirement in the handling of personal information. *The Data Protection Act 1998 (DPA)* specifies eight principles (see section 2) which must be observed by all employees, students or others dealing with personal data* on behalf of Northampton College. Both computer and manual records, including filing systems, employee files, Human Resource Information System (HRIS), MIS, eILP's, the electronic Document Management System and School student trackers are covered.

*Terms marked with an asterisk are defined in Appendix 1.

Although this policy concentrates on the *DPA*, Appendix 2 identifies other associated legislation.

2. KEY PRINCIPLES RELATING TO THE USE OF DATA

1 fairly and lawfully processed;

2 processed for limited purposes;

3 adequate, relevant and not excessive;

4 accurate and up-to-date;

5 not kept for longer than is necessary;

6 processed in line with your rights;

7 secure;

8 not transferred to other countries without adequate protection.

3. SENSITIVE DATA

Sensitive data is information relating to the individual's:

- racial or ethnic origin;
- political beliefs;
- religious beliefs or beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- commission or alleged commission of any offence;
- safeguarding related issues.

The DPA gives additional protection to sensitive personal data over and above that given to other personal data.

To fairly and lawfully process <u>sensitive</u> personal data at least one of the conditions below must be met:

- the explicit consent of the data subject (i.e. the person the data relates to) has been freely given;
- the processing is necessary for equal opportunities monitoring.

4. THE DATA CONTROLLER*

Northampton College is the data controller under the DPA. However the Head of Information and Services (HIS) will deal with day-to-day matters relating to students and the Director of Human Resources for employees.

In matters of collaboration and partnership with other bodies it is possible for either or both organisations to be the data controller, depending upon the nature of the agreement or contract. Please refer any queries to the HIS.

Failure to comply with the Act renders the Data Controller (Northampton College) liable for prosecution. In the case of an organisation like the College, an employee as well as the organisation may be liable for prosecution.

5. NOTIFICATION OF DATA* HELD AND PROCESSED*

Northampton College undertakes to maintain an accurate and timely notification of its data processing activities with the Office of the Information Commissioner (OIC). Copies of registration are available from the HIS. Maintenance of the notification is the responsibility of the HIS.

6. RIGHTS TO ACCESS INFORMATION

The College must respond to an access request promptly which is taken to mean as quickly as we reasonably can. It must, in any case, respond within 40 days of receipt of the request, or within 40 days of receipt of the information we require to satisfy ourselves about the identity of the person making the request (20 days for FOI).

In general the College works to a service standard of arranging for an employee's or student's request to be satisfied within 20 working days for employees of receiving the written request. This standard will only be extended if there is good reason to do so, for example other work pressures within the Department that make it impossible to meet the standard. If this is the case the requester will be contacted.

The College will only ever release information to a third party if it can be certain that the request is properly authorised by the subject (authority to divulge).

7. STUDENTS' ACCESS TO INFORMATION

College learning agreements and various student publications provide guidance to students regarding information disclosure or requests. See APPENDIX 3 for student data processing notice.

Students are entitled to request access to data about themselves whether it is held in a computer or in paper form. As personal data includes any expression of opinion about an individual, if we hold any adverse comments about students in relation to performance, for example, this is included in the right to access.

All student requests need to be made in writing (letter, email or fax) to the Data Protection Officer, via Student Data Services, Booth Lane.

When the College makes arrangements for a student to see his/her personal information the College will provide everything that existed at the date the request was made and will not make any special alterations to data to make it more acceptable. However, sometimes routine data may result in it being amended or even deleted whilst the College is dealing with the request and in that case it is reasonable for the College to supply the information available when at the point the response is sent.

The Act requires the College to provide the information to the student in an 'intelligible form', which the average person is capable of understanding. The Act does not require the College to ensure it is intelligible to the student e.g. a register mark key would be supplied with register information, but the College would not decipher poorly written notes.

When a student requests his/her data the College does not consider it practical to copy all the details in the personal file so will arrange a time when the student requesting can visit the Student Data Services Office and view the contents in the presence of either the Student Data Services Supervisor or Head of Information Services. Viewing files will take place at a convenient time and any documents the student requires will be copied.

8. STUDENT DOCUMENTS NOT ALLOWED TO BE SEEN

Information requests regarding student data will not be complied with if to do so would mean disclosing information about another individual who can be identified from the requested information or if they could be put at risk (see s7.3 'Working with students'). Exceptions will be made if the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply.

9. EMPLOYEES' ACCESS TO INFORMATION

The College 'Staff Handbook' provides guidance to employees regarding the processing of their personal data and information about disclosure requests. See Appendix 5.

Employees are entitled to request access to data about themselves whether it is held in a computer or in paper form. If an employee wants to see what information is held by the Human Resources Department, a written (letter, email or fax) request must be submitted, addressed to the Director of Human Resources.

As personal data includes any expression of opinion about an individual, if we hold any adverse comments about employees in relation to performance, for example, this is included in the right to access.

When the College makes arrangements for an employee to see his/her personal file the College will provide everything that existed at the date the request was made and will not make any special alterations to data to make it more acceptable.

There are some exceptions to the information that will be made available defined in the section 10 of this policy.

When an employee requests his/her data the College does not consider it practical to copy all the details in the personal file so will arrange a time when the employee requesting can visit the Human Resources Department and view the contents in the presence of one of the Human Resources staff. Viewing files will take place at a convenient time and any documents the employee requires will be copied and either sent or handed to the employee where this is impossible, the College will agree with the requesting employee how the data will be provided.

10. EMPLOYEE DOCUMENTS NOT ALLOWED TO BE SEEN

In certain circumstances, access to particular documents may be restricted. The Human Resources Department might restrict access under the following circumstances:

- where access to the document would or could cause interference with a current investigation by the College;
- where documents contain information dated prior to 1 March 1996 which was provided on the understanding that such information would remain confidential;

Any confidential documents will be sealed by a member of Human Resources staff but a list of these documents will be provided.

11. DATA SECURITY: DEALING WITH THIRD PARTY ENQUIRIES

Northampton College is committed to data security and will make every effort to safeguard against illegitimate disclosure of personal information. Where a request for personal information is received from a third party, the request needs to be promptly forwarded to Student Data Services (SDS) or to Human Resources (HR) as appropriate. SDS or HR will then ensure the request made by the third party meets DPA requirements before disclosure is even considered (see Appendices 4 and 5). Third party enquiries/requests also include the Police. Police requests should be directed to Student Data Services or Human Resources if appropriate, who will also inform the Principal's Office and the Safe Guarding Officers where appropriate.

12. REFUSALS TO SEE INFORMATION HELD

Under the Act the College is not compelled to comply with a request that is similar or identical to a request made previously, unless a reasonable interval has passed since the previous request was made. This provision will only be relied upon when it is absolutely necessary and needed to protect Human Resources or Student Data Services staff from being overstretched in the discharge of their other duties.

13. THE COLLEGE'S RESPONSIBILITY FOR DATA HELD ABOUT EMPLOYEES AND STUDENTS

The College has a duty to ensure that the information held is accurate. In addition the College can only hold information which is necessary.

I. Human Resources

Members of the Human Resources Department will:

- only request and record information about employees, or prospective employees that is appropriate to the recruitment process and ongoing management of the employment relationship;
- only access and process the information that is necessary to perform the duties of the job;
- ensure information is kept up to date and is accurate;
- ensure information is updated at appropriate times e.g. disciplinary details which are considered inactive after a certain period of time;
- maintain the security of information by keeping passwords confidential and locking records away;
- Not access information purely for personal interest.

II. All College Employees

i. Awareness& responsibilities

All employees will need to be aware:

- of the basic concepts as outlined in this policy and follow them where appropriate;
- that all personal data collected, held, and processed, on computer and on-line, are subject to the *Data Protection Principles and should only be collected if really necessary (nothing should be either requested or recorded on the grounds that "it might come in useful", neither should it be used for purposes inconsistent with those specified in the College Data Registration document);
- that extra care should be taken in the handling and storage of *sensitive personal data;
- that all personal data collected held and processed in structured manual files are subject to the *Data Protection Principles;
- Of the circumstances under which they may legitimately access, process or disclose personal data whilst employed at Northampton College.

All employees must ensure that:

- processing of personal data must be for a purpose that is explicit, lawful and covered by the College's notification;
- When processing personal data (whether on or offsite) clear processes must exist by which any individual access requests can be satisfied appropriately i.e. records can be easily obtained when DPA requests are made.

ii. Storage of data by employees

Precautions should be taken to prevent any unauthorised access to personal data. Any information relating to named individuals should be handled and stored securely:

- desks or filing cabinets should be locked;
- computers should be password-protected and passwords not disclosed to others;
- data storage devices containing personal information should be kept safe;
- papers should not be left out on desks or tables;
- information on computer screens should not be accessible/visible to other than authorised users;
- *sensitive data should be secure and subject to very limited access using password protection;
- personal data should not be removed from the College or stored elsewhere unless such use is recognised and authorised;
- remote access to secure, on-line College information should be used wherever possible as an alternative to taking personal data off-site;
- computers and data storage devices taken off-site should not be left unattended in vehicles;
- laptop computers and data storage devices should be encrypted if they are to be taken off-site holding personal data – see the ICT Security Policy;
- off-site security must conform to College standards as outlined above.

To minimise the risk of personal data being mishandled it is recommended that information be held in one file wherever possible, rather than being dispersed or duplicated in several places. For example, material concerning current learners should be held on file in the School Office with the maintenance of separate files by tutors being avoided as far as is practicable and possible. Data should not be held indefinitely.

iii. Disclosure of information

No information should be given to any third party without permission of the employee or student. This includes parents or other relations (unless the specified next of kin provided at enrolment for learners aged under 19), partners, friends, colleagues, fellow learners.

College procedures may be discussed freely with anyone. Thus it is possible to explain to a parent what, *in principle*, happens when a student must retake examinations, spend time on work placement, etc but not to divulge the specific circumstances of an individual's case without the agreement of that student. See section 7.3 of 'Working with students' for more in-depth guidance.

You may find yourself being asked by an individual to give them information in accordance with the Act. If so, you should not attempt to deal with it yourself, but should refer the enquirer to Student Data Services or Human Resources as appropriate. All DPA requests concerning students, including student references (excluding UCAS), Council Tax requests, government agency requests (Department for Work and Pensions, Home Office, Immigration Services etc), Employment Agency Requests, Solicitors Requests and Police Requests, are centrally recorded by the Student Data Services team and clarification is sought from the Head of Information Services (HIS). All DPA requests concerning employees should be referred to the Human Resources department. These may include requests from government agencies, building societies, solicitors, property landlords and partner organisations.

The Head of Information Services is the Northampton College Data Controller Representative for all College data collected and processed.

iv. Providing student references

All reference requests need to initially go through Student Data Services. They will contact the relevant tutor using a standard proforma to collect the information required. When supplying a reference, it should be assumed that the student will have the right to read it. Information should be factual and verifiable with unsubstantiated opinion being avoided. For further information relating to reference requests please see Appendix 4 s5.

v. Providing staff references

Requests for staff references should be prepared in line with the College Staff Reference guidelines on the Document Library then sent to HR for final preparation and issue. It should be assumed that the employee will have the right to read it. Information should be factual and verifiable with unsubstantiated opinion being avoided.

vi. Disposal of information

Records must be disposed of securely through shredding or incineration to ensure no accidental disclosure to any third parties. See section 17 for further details

vii. Employee personal data and requirements

Employees must keep their Line Manager and Human Resources Department advised without delay if any of their personal details change. This will enable records to be kept up to date and avoid difficulties later if action is required by the College, for example, sending letters to home addresses.

III. Students

All students are responsible for:

- checking that information they provide to Northampton College in connection with their membership of the College is accurate and up-to-date;
- advising Northampton College of any amendments to this information, e.g. changes of address. They can update their address details via Moodle (e-ILP) or by visiting the Student Data Services Office.

It is College practice to send all external awarding body certificates to a student’s home address or where appropriate direct to an external training broker. If a student has not advised the Exams/Student Data Services Office of a change of address, the College would normally expect the student to pay for their replacement (regardless of age and fund stream). If a certificate is returned the College provides the student with the option of resending to their revised address or for them to collect in person. There is Exams Manager discretion for exceptional circumstances.

Northampton College cannot be held responsible for any errors unless the student has provided updated information as here requested.

Please see Annex 3 for ‘Data Processing Notice to Students’.

14. BREACHES OF THE *DATA PROTECTION PRINCIPLES AND WORK PRACTICES

Not following the standards and work practices set out by the College will be a breach of the Data Protection Principles and the person in breach would be seen as accessing data that was not for a 'specified and lawful' reason.

Anyone who considers that the practices have not been followed in respect of personal data about him/herself should discuss the matter with his /her line manager, or in relation to students their tutor, in the first instance. Any alleged breach will be investigated and where appropriate disciplinary action will be taken. Serious cases might result in the person who had accessed data in breach of this policy being dismissed.

15. IT TRAINING AND ACCESS TO COLLEGE STUDENT RELATED SOFTWARE

All employees will need to sign an Acceptable Use Policy document before they are able to access the College network. Please refer to Human Resources for further details.

The College has a variety of software relating to students including QL, Pro-Achieve, Goldmine, QL Reports, QL-e, Tokam,Tok Open–Document Management System. Training on the use of student-related software is encouraged prior to software permissions being given.

16. USING INFORMATION FOR RESEARCH

I. Employee research

Employees and, where relevant, students engaging in research as part of their studies, will be covered by Northampton College's Data Protection Notification. Research undertaken should not be published in a way that:

- would identify or is targeted towards individuals or cause them damage or distress;
- would support measures or decisions with respect to particular individuals.

Data used for research purposes has certain exemptions from the terms of the DPA. In practice, this means:

- *the second principle* – *personal data 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 purposes;* **(Personal data can be processed for research purposes other than which they were originally obtained.)**
- *the fifth principle - personal data for any purpose or purposes shall not be kept any longer than necessary for that purpose or purposes.* **(Personal data processed for research purposes may be held indefinitely.)**

These exemptions allow the College to choose to disclose the information to the data subject, unless by doing so they would breach another individual's data protection rights.

Despite the terms of these exemptions, Northampton College seeks to ensure that, wherever practicable, data subjects are made fully aware of any research for which their personal data may be used. Researchers are required to keep their data secure and to guard against any accidental disclosure that might arise from direct or indirect reference to individuals in any research report.

II. Student research

Students who need to process personal data as a justifiable part of their course will be covered by Northampton College's Data Protection Notification. They will be expected to observe the relevant guidelines issued by the College. Should they be processing on behalf of another organisation, whilst on placement for example, they will be bound by the Data Protection policies and provisions of that organisation.

III. Provision of research data to third parties

These requests fall under the *FOIA. All FOIA requests must be dealt with by the Principal's Office. Before any information can be disclosed the following points need to be considered:

- whether the specific data requested, or from the data requested combined with additional information available from other sources, may contain or allow the identification of personal data; *(In such cases the College could consider a statistical form to eliminate this risk.)*
- whether the cost of providing the data in an appropriate format is reasonable on grounds of cost.

17. RETENTION OF DATA

N.B. A current and more detailed list of the required retention periods for records is maintained by the Finance department.

I. Student Data and information

In general, detailed information about learners will be kept by the Student and Information Services Directorate for a maximum of seven years after they leave Northampton College. Please see table below.

Type of record	Suggested retention period	Reason for length of period
Safeguarding	Minimum of 7 years	Legislation
Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence	Limitation period for negligence
ESF Student records, including academic achievements and conduct	Scanned copy of full student records including documents relating to: - application/admission - transfer, withdrawal or termination of studies - academic achievements 7 years after the final payment under the programme (e.g. 2022 for the 2009-2015 funding programme).	ESF funding requirements (for potentially ESF matched funding)
	At least 10 years for personal and academic references	Permits institution to provide references for a reasonable length of time
	Certain personal data may be held in perpetuity	While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data

This data will be a combination of paper, electronic and scanned images.

Records must be disposed of securely through shredding or incineration to ensure no accidental disclosure to any third parties. Please refer to the Director of Finance Secretary with regard to outsourcing of sensitive data disposal.

II. College Schools – Student information

In general, detailed information about students will be kept by Schools for a maximum of 6 years after they leave Northampton College. This will include:

- biographical details;
- assessments records;

- progress trackers;
- progress reports;
- ILPS;
- interview records;
- disciplinary records;
- written informal warnings;
- team minutes;
- e-mails referring to individuals.

III. **HR – Employee information**

Whilst there is clear guidance about some information in statute, the College will hold information while it is relevant to do so, (i.e. about an existing employee) or to protect the organisation in the event of a challenge being made. The table below sets out the timescales for each piece of information against the statutory minimum times where they exist.

Record	**Statutory Retention period**	**College's Policy**
Statutory Maternity pay records, calculations and certificates, etc.	3 years from the end of the financial year the maternity occurred in	6 years
Statutory sick pay records, calculations and certificates and self-certificates	3 years from the end of the financial year they relate to	6 years
Wage/salary records, overtime, etc	6 years from the end of the employment	Same
Application forms and interview notes for unsuccessful candidates	None	1 year
Parental leave records	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance	6 years
Personnel files and disciplinary records	None	6 years from the date employment ceases
Redundancy details	None	6 years from the date of redundancy
Senior executives records	None	Permanently for historical purposes only
Employment references received	None	6 months
Pension records	None	Kept until retirement age.

18. CCTV

The College operates a CCTV monitoring system on all sites. The purpose of this system is to:

- assist in the detection and deterrence of crime;
- provide evidence of crime;
- give confidence to students, staff and visitors that they are in a safe environment;
- provide management information with regard to health and safety;
- provide management information to assist in the operation of College policies;
- provide information with regard to traffic management;
- to assist the Police and civil authorities in the event of a major emergency. The system will be operated in such as way as to safeguard individuals' right to privacy.

Please see the CCTV Policy Statement available on the College Document Library for further details.

19. PRIVACY IMPACT ASSESSMENT (PIA)

When the College considers adopting a new administrative system and other processes with possible privacy implications, or updating existing systems or processes (such as MIS, HRIS, VLE's, E-Portfolio and distance learning programmes), the appropriate employees must undertake a PIA in the early stages of the project and before implementation. Potential privacy issues and risks must be identified. Guidance on PIA's, including when a PIA should be carried out, who should be involved, and what form the process might take, is available from the ICO website at:

http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

20. FURTHER INFORMATION

Other relevant information available on the Document Library includes:

- Staff Disciplinary Policy;
- Student Disciplinary Policy;
- ICT Security Policy;
- ICT Acceptable Use Policy;
- CCTV Policy;
- Safeguarding Children and Vulnerable Adults Policy;
- "Working with Students" guidelines;
- Staff Reference guidelines.

Further information on Data Protection legislation may be found on the following external website:

Office of the Information Commissioner http://www.ico.gov.uk/

Please refer any employee data queries to the Director of HR and student data queries to the Head of Information Services.

21. CONCLUSION

Compliance with the DPA is the responsibility of all employees of Northampton College. Any deliberate breach of the Data Protection policy may lead to disciplinary or even a criminal prosecution.

Appendix 1 Glossary of data protection terms

Data… is defined under the DPA 1998 as follows:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filing system or within the intention that it should form part of a relevant filing system;
- is not covered by the first two categories but forms part of an "accessible record" e.g.:
  - a health record consisting of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection of the care of that individual;
  - an educational record processed by or on behalf of the governing body of, or a teacher at, any school in England or Wales which relates to any person who is or has been a pupil at the school, and originated from or was supplied by or on behalf of an employee of the local education authority which maintains the school, a teacher or other employee at the school, the pupil to whom the record relates or the parent of that pupil;
  - any accessible public record that is kept by an authority specified in Schedule 12 of the DPA 1998.
- is recorded information held by public authority and does not fall into any of the previous categories.

Data Controller: the person/people who determine(s) the purposes for which, and the manner in which, personal information is to be processed and whose duty it is to ensure that the Data Protection Principles are applied. In the context of this institution the Data Controller is Northampton College.

Data Processor: is any employee of Northampton College.

Data Subject: any living individual who is the subject of personal information. People who have died cannot be data subjects, nor, in the UK and most other EU member states can "legal individuals" such as companies.

Fair Processing Notice: is used by Northampton College to provide data subjects with information about the processing of their personal data, usually at the time of its collection. It will describe the purposes for which Northampton College intends to process their personal data and will include details of joint data controllership, as well as third parties to who data may be disclosed or transferred, and the purposes served by those transfers or disclosures.

Northampton College examples found on the Enrolment/Student Agreement:

- display boards – to inform students of college related activities;
- parent/guardian evenings;
- disciplinary/grievance procedures;
- attendance monitoring;
- correspondence to students relating programme of study;
- distribution examination/registration documents;
- storage and usage of student image used to create ID cards;
- disclosure to government agencies/Police within the confines of legislation;
- contact to learners via text, email or post using information collected on the enrolment/student agreement.

In relation to the enrolment/student agreement the disclosure to third parties includes disclosure to: the Department for Children, School and Families; the Department for Innovation; Universities; Skills/Connexions/Higher Educations Statistics Agency.

For prospective and existing staff the Human Resources department provides data subjects with information about how their data will be used and processed and the purposes for which it is collected. Examples are found on:

- on-line and manual Job Application Forms;
- contracts of employment.

Inaccurate Data: data which is incorrect or misleading as to a matter of fact.

Notification: entry on the public register maintained by the Information Commissioner's Office showing types and range of information being processed by the college.

Personal Data: information about a living individual who can be identified from that information or from other information that is in, or is likely to come into, the possession of the College. The data has biographical significance in relation to the living individual. The data impacts or has the potential to impact on an individual whether in a personal, family or professional capacity.

Processing: obtaining, recording or holding information or carrying out any set of operations on it. This includes collections, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. It is irrelevant whether these actions and manual or automated. The use of QL-e, QLV4, Tok-Open, Tokam, QLS Reports, Pro-Achieve, Human Resources Information System, eILP's and School Student Trackers are forms of data processing.

Appendix 2 DPA Interaction with other associated legislation

The Freedom of Information Act 2000 (FOIA 2000) and Freedom of Information Scotland 2002 (FOISA 2002)

The FOIA's give a general right of public access to all types of "recorded" information held by public authorities, sets out exemptions from that general right, and places a number of obligations on public authorities. Therefore these Acts include schools, colleges and universities. So the FOIA's and DPA relate to aspects of information and they overlap where personal information is considered for disclosure. Northampton College has two main responsibilities under the Acts:

- the College must produce a publication scheme, (This guide which details information held which is publicly available can be found in http://www.northamptoncollege.ac.uk/aboutus/documents/publicationscheme_doc.pdf.)
- the College must deal with individual public requests for information. The FOIA and the FOISA, in addition to access to an individual's personal data (held on computer and paper files) permit individuals to request all other types of information that public authorities hold (subject to specific exemptions in the acts).

All FOIA requests must be forwarded to the Principal's Office in a timely manner. Individual employees must not reply in person.

NB: if a request is made by an individual for information about him or herself, it should be handled under the DPA 1998. All requests (including student and staff references) must be forwarded to Student Data Services or to the Director of Human Resources as appropriate.

Human Rights Act 1998

The main provision of the Human Rights Act 1998 relevant to data protection is Article eight, which states:

- everyone has the right to respect for his private and family life, his home and correspondence;
- there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

Therefore, breaches of the DPA 1998 could give an indirect cause of action to individuals seeking to claim their Article eight rights were being breached.

Regulation of Investigatory Powers Act (RIPA) 2000

This provides, in conjunction with the Telecommunications Regulations 2000 (Lawful Business Practice & Interception of Communications), grounds for the lawful interception of communications, including telephone and computer communications. However, personal data collected under RIPA 2000 and LBPR must be processed in accordance with DPA 1998 requirements, unless elements of that processing are specifically exempted for the purposes of law enforcement, s.29, DPA 1998 or national security (s.28, DPA 1998).

Privacy and Electronic Communications Regulations 2003 (PECR 2003)

This EC directive regulates direct marketing activities by electronic means (phone, fax, email etc). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and spyware. The regulations compliment the DPA 1998 in the regulation of organisations use of personal data and ensure appropriate safeguards for individuals' rights and privacy.

Where personal data is used the DPA 1998 always applies and the regulations cannot be used to avoid DPA requirements.

Electronic Commerce Regulations 2002

This EC directive aims to ensure that individuals are able to effectively utilise consumer protections and other rights, including those granted under the DPA 1998 and the PECR 2003 by providing them with the necessary information about whom to enforce those rights.

Appendix 3 Student Privacy notice 2011-2012

Northampton College is notified as a data controller with the Office of the Information Commissioner and collects and processes information about students for various teaching, funding and administrative purposes. All such activity is governed by the Data Protection Act 1998 and students are entitled to have access to the records held about them.

The College allows employees of the College to access data on a strictly need-to-know basis.

Student information is used for the following purposes:

- display boards (including digital display) – to inform students of college related activities;
- parent/guardian evenings;
- disciplinary/grievance procedures;
- attendance monitoring;
- correspondence to students relating programme of study;
- distribution examination/registration documents;
- storage and usage of student image used to create ID Cards;
- contact to students via text, email or post using information collected on the enrolment/learning agreement;
- the provision of advice and support to learners via, amongst others, Student Data Services, Student Services and Additional Support;
- registration with awarding bodies;
- ULN number creation;
- Safeguarding;
- disclosing information to the Local Authority;
- disclosing information to sponsors/employers (where stated on the Learning Agreement)
- disclosing information to current external work based training providers;
- disclosing information to professional and statutory bodies;
- disclosing information to government agencies including the Police, if deemed necessary and within the confines of legislation. In particular in relation to safeguarding of young people and vulnerable adults and others and in line with the Children's Act and FE Act.

- Disclosing information to funding agencies:
    - The personal information you provide is passed to the Chief Executive of Skills Funding ("the Agency") and, when needed, the Young People's Learning Agency for England ("the YPLA") to meet legal duties under the Apprenticeships, Skills, Children and Learning Act 2009, and for the Agency's Learning Records Service (LRS) to create and maintain a unique learner number (ULN). The information you provide may be shared with other partner organisations for purposes relating to education or training.

      Further information about use of and access to your personal data, and details of partner organisations are available at:
      http://skillsfundingagency.bis.gov.uk/privacy.htm
      http://www.ypla.gov.uk/privacy.htm
      and
      http://www.learningrecordsservice.org.uk/documentlibrary/documents/Code+o+f+Practice+for+Sharing+of+Personal+Information.htm

- Disclosing information on your learning status including – attendance, awarding body entry and exam attendance, if you are a 16-18 year old student (at the start of your learning programme). This data will only be disclosed to the next of kin(s) (i.e. parent/guardian) details you provided at enrolment. If parental/guardian details change during your time at Northampton College, please contact Student Data Services. Student support payments will **NOT** be discussed with next of kin;
- Students have the right to request that the College does not disclose any personal information to parents/guardians.

The accuracy of personal information provided by students may also be checked by the College against relevant external sources such as the YPLA or SFA.

The College undertakes to maintain student data in secure conditions, and to process and disclose data only within the terms of its Data Protection notification. The details above indicate the nature of this notification but are not exhaustive.

Please note that we are reliant on you for much of the data we hold. Help us keep your record up-to-date by notifying us of any alterations to your address, personal details, next of kin or course details. This can be done (depending on the amendment) via Moodle/E-ILP, Student Data Services or your tutor.

Please contact Student Data Services, H Block, Booth Lane, if you have any specific questions relating to Data Protection or for details of procedures relating to your rights as a data subject.

Appendix 4 Staff Guidelines for the disclosure of student personal data

1. Introduction

Northampton College receives regular requests for information on students, both past and current. Please do not hesitate to contact Student Data Services (SDS) should you need any further information or explanation.

The main thing to remember is that, according to the Data Protection Act 1998 (DPA), there is limited disclosure of personal information without the data subject's (student's) authorisation.

2. Disclosure overview

Please note any request should be referred to Student Data Services and/or the Information Services Manager.

Student Data Services/Head of Information Services:

- will check students have a signed learning agreement;
- will deal with requests promptly (as per the legislation and our service level) but before responding will ask for information that reasonably would be needed to find the correct data (the 40 day response time does not begin to run until Student Data Services has received any additional information required);
- will ascertain whether the person making the request relates to the information they require;
- will verify individual requests received from third party organisations/bodies listed below; (They must be made in writing on official headed paper and should ideally cite the relevant DPA exemption or other legislation which authorises the College to release the information, or provide a signed declaration of authority to divulge information.)
- will verify individual requests received from third party on behalf of an individual (student) by ensuring a signed declaration is provided (if the College feels the student concerned may not understand what information may be disclosed to the third party, we could chose to send the response directly to the student. The student can then choose to share the information after having the chance to read it.);
- will not comply with a data request if to do so would mean disclosing information about another individual who can be identified from the requested information (exceptions will be made if the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply);
- will provide information in a permanent form unless it would involve disproportionate effort to do so. (In this case, we would invite the student to visit to view the original documents and copy any documents they would like to take away. Any visit will be in the presence of either the Student Data Services Supervisor or Head of Information Services.)

3. Exceptional circumstances for disclosure

Confidentiality may have to be breached if there is a danger that:

- the student may harm him/herself;
- the student may harm other persons;
- the student's life or health or safety may be threatened.

Please refer to the Director of Student Services or any of the College designated Safeguarding Officers if these circumstances arise.

Sections 4 - 10 below show who might request student information from the College either as a regular or ad hoc occurrence.

4. Disclosure to Families/Relatives

The College is not under any obligation to provide information to relatives without consent. Although employees may come under pressure to discuss learners' cases with parents, it is essential that personal information is not disclosed without the written or verbal consent of the student involved.

Exception:

All students provide 'next of kin' details at point of enrolment. If the student is aged under 19 at start of their Learning Programme, the College will provide information to those persons relating to the student's learning status including attendance, awarding body entry and exam attendance unless the student has formally requested the College not to. If next of kin details change during the course, learners must contact Student Data Services. This potential disclosure is made clear on learning agreements and in student publications.

College procedures may be discussed freely with anyone. It is possible to explain to a parent what, in principle, happens when a student must retake examinations, go on work placement, apply for Additional Support, etc but not to divulge the specific circumstances of an individual's case without the agreement of that student.

5. Disclosure to third parties or student requests for a student reference

All reference requests other than UCAS ones will be actioned by the Assistant Liaison staff in the Student Data Services Office.

If a student asks any employees to provide them with a reference the student must be directed to Student Data Services where a reference request form will be completed.

Student Data Services will only provide references to individual companies or organisations; we cannot provide "to whom it may concern" letters. If a reference is being requested by the student they will need to provide the name and address of the company/organisation for which the letter is intended.

When the Assistant Liaisons receive a reference in the post that requires a personal opinion by the tutor they will send a standard email form direct to the tutor concerned. The tutor should complete the reference and send the email response back within 5 working days.

Requests will only be provided where a student's signed authority to divulge is available.

The Student Data Services service standard for 'full' references is 15 working days.

6. Disclosure to the Police

Disclosures to representatives of the Police are not compulsory except in cases where the institution is served with a court order requiring information. However, the DPA does allow exemption in cases where data is disclosed in relation to "the prevention or detection of crime" and "the apprehension or prosecution of offenders".

The College may choose to release personal information to the Police in limited circumstances. Such disclosures should be made only in cases where the Police confirm that they wish to contact a named individual about a named criminal investigation, regardless of whether that individual is suspect or witness, *and where we are reasonably satisfied that failure to release would prejudice the investigation*.

Information should be provided only on receipt of written confirmation or College Proforma with the signature and badge number of the investigating officer. This should always include a statement confirming that the information requested is required for the purposes covered in Section 29 or other relevant section of the Act/Legislation.

The request should be explicit as only specific data will be issued.

Any release should be reported to the Head of Information Systems with an Executive Management Team member's signature. The Principal's Office should also be informed and the Safeguarding Officer where appropriate.

All Police requests will be entered on the institutional Exceptional Disclosures Log by the Principal's Office.

7. Disclosure to Government agencies

i. Her Majesty's Revenue and Customs (HMRC)

Disclosures should be made when an official written application is received from HMRC in relation to the collection of tax or duty. The relevant DPA exemption, normally section 29, should be quoted.

Any release should be reported to the Head of Information Systems and Principal's Office for entry in the College Exceptional Disclosures Log.

ii. Home Office/Home Office Border and Immigration Agency

There is a statutory obligation to co-operate when enquiries are received from the Home Office. The request should be made in writing on official paper and it is best practice for the relevant exemption to be quoted.

Any release should be reported to the Enrolment Centre Manager (if relating to Admissions) HIS (if relating to Enrolled Learners) and Principal's Office for entry in the institutional Exceptional Disclosures Log.

The College must follow the Border Regulations which includes disclosing overseas students' College status and attendance. Please refer to the Enrolment Centre Manager if you receive these requests.

iii. Child Support Agency (CSA), Financial Services Agency (FSA)

There is a statutory obligation to co-operate when enquiries are received from the CSA/FSA. The request should be made in writing on official paper and it is best practice for the relevant DPA exemption to be quoted.

Any release should be reported to the HIS and Principal's Office for entry in the College Exceptional Disclosures Log.

iv. Department for Work and Pensions (DWP)/Jobcentre plus

In cases where an officer of the DWP suspects an individual of benefit fraud, statutory powers are available to them to require the College to provide data on one or more named individuals. Written statements should be obtained from the relevant authorised Officer explaining the reason for the request.

Any release should be reported to the ISM and Principals Office for entry in the institutional Exceptional Disclosures Log.

v. Health and Safety Executive (HSE), Department of Health/Environmental Health Officers, Environment Agency, College Insurers (relating to student accidents)

Please refer all requests made by the above agencies to the College Director of Estates or the Health & Safety Officer.

vi. Higher Education Funding Council for England (HEFCE) and agents such as Higher Education Statistics Agency (HESA) and HEFCE auditors

The College is required by law to disclose information to the Higher Education Funding Council for England on request. This includes the incidental disclosure of student data during visits by academic or other auditors appointed by the Funding Council. Disclosures may also be made to agents of the Funding Council.

This is explained in the Data Protection statement on the College Enrolment/Learning Agreement.

vii. National Health Service (NHS) Fraud Investigators

Official requests received in writing and which cite the relevant DPA exemption to permit disclosure should normally be met.

8. Disclosure to College Related agencies

i. Internal and External Auditors/OFSTED

The College is required by its own statutes (and funding bodies) to appoint external auditors. It is acceptable that such auditors will inevitably see student data (via controlled access) during the course of their investigations.

ii. Sponsors including Training Providers

The College is under no obligation to provide information to sponsors/employers without consent. Consent is gained via the College Learning Agreements or International Student agreements.

If consent has been gained the following information will be divulged:

- Progress/achievement;
- Attendance reports.

iii. UCAS

As applicants are made aware by UCAS when they first submit their details that information will be passed between them and the College, relevant data may be shared freely with UCAS as the need arises. For further information please refer to Student Support.

9. Disclosure to Local Authorities

i. Census

Census officers have no statutory right to ask the College to provide student data. The College should co-operate with the distribution of Census forms as far as is possible, but personal information should not be released directly to Census officers without prior permission from the student(s) involved.

ii. Council Tax Registration Officers

Student data *may* be disclosed to Council Tax Registration Officers as necessary, even without consent. The request must be made in writing and specify the exact provisions under which the request is made, normally section 29.

There must be reasonable grounds for believing that failure to disclose to these officers would adversely affect the collection of or assessment of any tax.

Any release should be reported to the HIS and Principal's Office for entry in the College Exceptional Disclosures Log.

iii. Electoral Registration Officers

Electoral Registration Officers have certain powers to require the provision of student information for the purposes of maintaining registers of parliamentary and local government electors.

If approached by an Electoral Registration Officer for information about learners, the College should check the reason for the request and under what legislative act. If satisfied with this, the disclosures can be made but learners should be informed of the disclosure.

iv. Social Services (Children and Vulnerable Adults) – including looked after children

All requests to go via the College's designated Safeguarding Officers. Please also see the Safeguarding policy. Approved regular student data updates will be made by SDS.

v. Teenage Parents Support Team (NHS)

All requests need to be made in writing for the attention of the Director of Student Services.

10. Disclosure to other organisations

i. Survey/research organisations

The College may be approached, from time to time, by survey and research organisations, or others conducting research, who wish to be provided with student information or contact details for a sample of the student body. The College *must* seek informed consent from any student whose details might be disclosed in this context.

ii. Other Educational establishments

The College may be asked for information about current or former students by other educational establishments. Requests for information from institutions formerly attended by the student should not normally be met, unless either the student has authorised the disclosure or the other institution can provide verifiable justification under the DPA.

iii. Employers and Recruitment Agencies

The College may be asked for information about existing or former students by current or potential employers and recruitment agencies. Evidence of authority to divulge is required before disclosure.

iv. Solicitors acting on behalf of other persons/bodies

The DPA's non-disclosure provisions are waived for the purpose of "or in connection with legal proceedings…or is otherwise necessary for…establishing, exercising or defending legal rights".

In cases where the College is approached by solicitors or others engaged in a Court case (not directly involving the College); it is College policy that any such requests should be directed to Student Data Services. Information will not be disclosed without the consent of the student concerned.

If requests are received which directly involve the College, please inform the Principal's Office.

Appendix 5 Staff Privacy Notice

Northampton College is notified as a data controller with the Office of the Information Commissioner and collects and processes information about staff for various teaching, funding and administrative purposes. All such activity is governed by the Data Protection Act 1998 and staff are entitled to have access to the records held about them.

The College allows employees of the College to access data about colleagues on a strictly need-to-know basis.

Staff information is used for the following purposes:

- the purpose of the recruitment and selection process;
- to support the administration processes underpinning the employment of staff;
- to support the College in the operation of its Policies;
- to enable the College to monitor the effectiveness of College Policies;
- to assist with statistical returns to funding bodies and government agencies;
- to assist with College internal and external audit requirements;
- to ensure compliance with employment law;
- disclosing information to government agencies including the Police, if deemed necessary and within the confines of legislation, in particular in relation to safeguarding of young people and vulnerable adults and others and in line with the Children's Act and FE Act;
- disclosing information to funding agencies:
  - the personal information you provide is passed to the Chief Executive of Skills Funding ("theAgency")
  - The information you provide may be shared with other partner organisations for purposes relating to education or training.
  - Further information about use of and access to your personal data, and details of partner organisations are available at: http://skillsfundingagency.bis.gov.uk/privacy.htm
- disclosing information to partnership organisations:
  - this is provided on receipt of a specific request from a partnership organisation and consent is sought from the employee before data is released.

Appendix 6 Staff Guidelines for the Disclosure of Staff Personal Data

1. Introduction

Northampton College receives requests for information on employees, both past and current. Please do not hesitate to contact the HR team (HR) should you need any further information guidance.

The main thing to remember is that, according to the Data Protection Act 1998 (DPA), there is limited disclosure of personal information without the data subject's (employee's) authorisation.

2. Disclosure overview

Please note that any request should be referred to the Human Resources team and/or the Director of Human Resources.

The Human Resources team/Director of HR:

- will deal with requests promptly (as per the legislation and our service level) but before responding will ask for information that reasonably would be needed to find the correct data (the 40 day response time does not begin until to run until Human Resources has received the any additional information required);
- will ascertain whether the person making the request is a valid recipient of the information they require;
- will verify individual requests received from third party organisations/bodies listed below; (They must be made in writing on official headed paper and should ideally cite the relevant DPA exemption or other legislation which authorises the College to release the information, or provide a signed declaration of authority to divulge information.)
- will verify individual requests received from third party on behalf of an individual (employee) by ensuring a signed declaration is provided (if the College feels the employee concerned may not understand what information may be disclosed to the third party, we could chose to send the response directly to the employee. The employee can then choose to share the information after having the chance to read it.);
- will not comply with a data request if to do so would mean disclosing information about another individual who can be identified from the requested information (exceptions will be made if the other individual has consented to the disclosure or it is reasonable in all the circumstances to comply);
- will provide information in a permanent form unless it would involve disproportionate effort to do so (in this case, we would invite the employee to visit to view the original documents and copy any documents they would like to take away. Any visit will be in the presence of either a member of the HR team or Director of HR.).

3. Exceptional circumstances for disclosure

Confidentiality may have to be breached if there is a danger that:

- the employee may harm him/herself;
- the employee may harm other persons;
- the employee's life or health or safety may be threatened.

Please refer to the Director of HR or, if appropriate, any of the College designated Safeguarding Officers if these circumstances arise.

Sections 4 - 10 below show who might request employee information from the College either as a regular or ad hoc occurrence.

4. Disclosure to Families/Relatives or other third parties

The College is not under any obligation to provide information to relatives or other third parties, such as landlords, building societies and casual enquirers, without consent. It is essential that personal information is not disclosed without the written or verbal consent of the employee involved. Such enquiries should be directed to the HR team who will contact the employee to pass on any enquiries.

5. Disclosure to potential employers: requests for an employee reference

College policy is to respond only to written requests for a reference and to reply in written form only. The DPA has an impact on the type of information which may be given and also on an individual's right to view data written about them. Requests for staff references should be prepared in line with the College Staff Reference guidelines (available) on the Document Library then sent to HR for final preparation and issue. It should be assumed that the employee will have the right to read it. Information should be factual and verifiable with unsubstantiated opinion being avoided.

Human Resources will normally only provide references to individual companies or organisations, very occasionally it may be appropriate to provide "to whom it may concern" letters, requests for these must always be directed to the Director of Human Resources before issue.

6. Disclosure to the Police

Disclosures to representatives of the Police are not compulsory except in cases where the institution is served with a court order requiring information. However, the DPA does allow exemption in cases where data is disclosed in relation to "the prevention or detection of crime" and "the apprehension or prosecution of offenders".

The College may choose to release personal information to the Police in limited circumstances. Such disclosures should be made only in cases where the Police confirm that they wish to contact a named individual about a named criminal investigation, regardless of whether that individual is suspect or witness, *and where we are reasonably satisfied that failure to release would prejudice the investigation*.

Information should be provided only on receipt of written confirmation or College Proforma with the signature and badge number of the investigating officer. This should always include a statement confirming that the information requested is required for the purposes covered in Section 29 or other relevant section of the Act/Legislation:

- the request should be explicit as only specific data will be issued;
- all requests for information regarding a member of staff should be directed to the Director of Human Resources;
- any release of information will be authorised beforehand by the Director of HR or, in their absence, a member of the Executive Management Team;
- the Principal's Office should also be informed and the Safeguarding Officer where appropriate;
- all Police requests will be entered on the College Exceptional Disclosures Log by the Principal's Office.

7. Disclosure to Government agencies

i. Her Majesty's Revenue and Customs (HMRC)

Disclosures should be made when an official written application is received from HMRC in relation to the collection of tax or duty. The relevant DPA exemption, normally section 29, should be quoted.

Any release should be reported to the Director of HR and Principal's Office for entry in the College Exceptional Disclosures Log.

ii. Home Office/Home Office Border and Immigration Agency

There is a statutory obligation to co-operate when enquiries are received from the Home Office. The request should be made in writing on official paper and it is best practice for the relevant exemption to be quoted.

Any release should be reported to the Director of HR and Principal's Office for entry in the College Exceptional Disclosures Log.

iii. Child Support Agency (CSA), Financial Services Agency (FSA)

There is a statutory obligation to co-operate when enquiries are received from the CSA/FSA. The request should be made in writing on official paper and it is best practice for the relevant DPA exemption to be quoted.

Any release should be reported to the Director of HR and Principal's Office for entry in the College Exceptional Disclosures Log.

iv. Department for Work and Pensions (DWP)/Jobcentre plus

In cases where an officer of the DWP suspects an individual of benefit fraud, statutory powers are available to them to require the College to provide data on one or more named individuals. Written statements should be obtained from the relevant authorised Officer explaining the reason for the request.

Any release should be reported to the Director of HR and Principal's Office for entry in the College Exceptional Disclosures Log.

v. Health and Safety Executive (HSE), Department of Health/Environmental Health Officers, Environment Agency, College Insurers (relating to staff accidents)

Please refer all requests made by the above agencies to the Director of HR and inform the College Director of Estates or the Health & Safety Officer.

vi. National Health Service (NHS) Fraud Investigators

Official requests received in writing and which cite the relevant DPA exemption to permit disclosure should normally be met. They should be directed in the first instance to the Director of HR.

8. Disclosure to College Related agencies

i. Internal and External Auditors/OFSTED

The College is required by its own statutes (and funding bodies) to appoint external auditors. It is acceptable that such auditors will inevitably see staff data (via controlled access) during the course of their investigations.

9. Disclosure to Local Authorities

i. Census

Census officers have no statutory right to ask the College to provide employee data. The College should co-operate with the distribution of Census forms as far as is possible, but personal information should not be released directly to Census officers without prior permission from the employee(s) involved.

ii. Council Tax Registration Officers

Employee data *may* be disclosed to Council Tax Registration Officers as necessary, even without consent. The request must be made in writing and specify the exact provisions under which the request is made, normally section 29.

There must be reasonable grounds for believing that failure to disclose to these officers would adversely affect the collection of or assessment of any tax.

Any release should be reported to the Director of HR and Principal's Office for entry in the College Exceptional Disclosures Log.

10. Disclosure to other organisations

i. Solicitors acting on behalf of other persons/bodies

The DPA's non-disclosure provisions are waived for the purpose of "or in connection with legal proceedings…or is otherwise necessary for…establishing, exercising or defending legal rights".

In cases where the College is approached by solicitors or others engaged in a Court case (not directly involving the College) any such requests should be directed to the Director of Human Resources in the first instance. Information will not be disclosed without the consent of the employee concerned.

If requests are received which directly involve the College, please inform the Principal's Office.

ii. Partnership organisations

Requests for information such as Curriculum Vitae should be submitted in writing and the purposes for which the information is required should be stated, along with the organisation representative responsible for the secure storage and legitimate use of the information in accordance with the DPA. Requests should be submitted to the Director of Human Resources in the first instance for authorisation.

The HR team will prepare the data, ensuring that no unnecessary personal information is included, notify the employee(s) of the disclosure and obtain their explicit permission to disclose it. The information will normally be encrypted to ensure its security when transferred electronically.