# http://staffhub.waltham.ac.uk/wfc_templates/Shared%20Documents/New%20WFC%20Logo%20Final%20-%20Black.jpg

# Data Protection Policy

|  |  |
| --- | --- |
| **Date of issue** | **November 2011** ***Updated September 2017*** |
| **Version** | **Version 4** |
| **Next Review** | **May 2018, or when required by legislation or the needs of the College if sooner (to incorporate new GDPR legislation)** |
| **Availability** | **Staff Intranet****On request from the Human Resources Department - including in larger typeface** |

**CONTENTS**

|  |  |  |
| --- | --- | --- |
|  |  | **Page No** |
| 1 | Purpose of the Policy | **3** |
| 2 | Policy Scope | **3** |
| 3 | Definitions | **3** |
| 4 | Principles | **3** |
| 5 | Notification of Data Held and Processed | **4** |
| 6 | Rights to Access Information and Disclosure | **4** |
| 7 | Responsibilities of Staff and Governors | **5** |
| 8 | Responsibilities of Students | **5** |
| 9 | Data Security | **5** |
| 10 | Publication of College Information | **6** |
| 11 | Processing Personal Data and Subject Consent | **6** |
| 12 | References | **7** |
| 13 | Retention and Disposal of Data | **7** |
| 14 | Designated Points of Contact | **7** |
| 15 | Review Arrangements | **7** |

|  |  |  |
| --- | --- | --- |
| Appendix 1 | Definitions | **8** |
| Appendix 2 | Staff Guidelines on handling personal information | **9** |
| Appendix 3 | Categories of personal information held on staff and students | **10** |
| Appendix 4 | Standard Request Form for access to data | **11** |
| Appendix 5 | Guidelines for Archiving | **12** |

1. **Purpose of the Policy**
	1. The purpose of the Policy is to ensure compliance with the Data Protection Act 1998.
	2. This Policy has been drafted with a view to balancing the legitimate needs of the College to collect and use personal data for business purposes against safeguarding the privacy rights of individuals in relation to the processing of personal data.
	3. This Policy is intended to ***protect*** staff and students and ***not*** to hinder you in your work.
2. **Policy Scope**
	1. This Policy applies to all Governors, students and staff (the term “staff” in this Policy includes agency workers, other temporary staff and volunteers).
	2. The College and all staff, or others who process or use any personal data or information, must ensure that they follow the principles of the Data Protection Act (see Section 4.2 below) and this Policy.
	3. For staff, this Policy does not form part of the formal contract of employment but it is a condition of employment that employees will familiarise themselves with and abide by the rules and policies of the College. Any failure to follow the Policy (eg passing data to a third party and/or using data for a purpose for which there is no authority) can therefore result in disciplinary proceedings.
	4. Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Head of Human Resources in the first instance or the College’s Data Protection Officer (Head of IT Services). If the matter is not resolved it should be raised as a formal grievance or complaint.
	5. Any questions or concerns about the interpretation of this Policy should be taken up with the College’s Data Protection Officer or the Head of Human Resources.
	6. This Policy should be read in conjunction with the College’s Freedom of Information Policy.
3. **Definitions**
	1. As with any legislation or policy, certain terms have particular meaning. A list of the important definitions is given in Appendix 1 to this Policy.
4. **Principles**
	1. The College needs to keep certain information about its employees, students and other users to allow it to undertake its business activities.
	2. To comply with the law, the College is required to take specific measures to ensure that personal data held about data subjects (or individuals) in either paper-based or electronic formats is processed according to eight Data Protection Principles, requiring that personal data must:
		1. be processed fairly and lawfully
		2. be obtained and processed for specific and lawful purposes only
		3. be adequate, relevant and not excessive for the specific purposes
		4. be kept for no longer than is necessary for the specific purposes
		5. be accurate and kept up to date
		6. be processed in accordance with the data subject’s rights and be provided to the individual on request
		7. be kept secure and safe from unauthorised or unlawful processing, accidental loss, damage or destruction
		8. not be transferred to a country or territory outside the European Economic Area without an adequate level of protection for the rights of data subjects
	3. As part of their responsibilities, some staff are required to collect personal information on students and/or staff. Where this is the case, the guidelines outlined in Appendix 2 of this Policy should be followed.
5. **Notification of Data Held and Processed**
	1. All staff, students and other users are entitled to know the following:
		1. what information the College holds and processes about them and why
		2. how to gain access to it
		3. how to keep it up to date
		4. what the College is doing to comply with its obligations under the Data Protection Act
	2. Appendix 3 of this Policy identifies the categories of personal information held by the College on staff and students.
6. **Rights to Access Information and Disclosure**
	1. Staff, students and other users of the College have the right to access any personal data being kept about them either on computer or file. The standard ‘Access to Information Form’ should be used (see Appendix 4).
	2. The College will make no charge that relates to personal data forming part of an accessible record or the first occasion that access is requested by an individual but reserves the right to make a charge of £10 (or other appropriate amount) for any subsequent request at its discretion.
	3. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 working days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request and this will be responded to within 40 working days.
	4. Disclosure to third parties is approved only on the following basis:
		1. With the written authority of the data subject
		2. In accordance with the College’s “Use of Personal Information and Consent Statement”
		3. When required by law or statutory instruction
		4. When required to prevent or detect crime
	5. In the case of 6.4.3 and 6.4.4 above any requests must be referred to the College’s Data Protection Officer or the Head of Human Resources and prior to any information being supplied to the authority making the request.
	6. The College’s Student Contract is based on the expectation that data (such as attendance and progress) will be shared with parents where the student is under 18 and/or employers if they are sponsoring the student at College.
7. **Responsibilities of Staff and Governors**
	1. Individual members of staff and Governors have a responsibility to:
		1. Check that any information they provide to the College is accurate and up-to-date
		2. Inform the College of any changes to the information they have provided in a timely manner.
		3. Check the accuracy of the information that the College will circulate from time to time which gives details of information kept and processed about staff.
		4. Inform the College of any errors or changes to information they are responsible for. The College cannot be held responsible for any errors unless the College has been informed of them.
	2. If and when, as part of their responsibilities, staff collect information about data subjects (eg about students’ course work, opinions about ability, references to other institutions, or details of personal circumstances), they must comply with the guidelines for staff (see Appendix 2).
8. **Responsibilities of Students**
	1. Students have a responsibility to:
		1. Ensure that all personal data provided to the College is accurate and up-to-date.
		2. Inform their Course Tutor or the Student Services Department (Room 219) of any changes to the information they have provided in a timely manner.
9. **Data Security (see also Appendices 2, 3 and 6)**
	1. It is a criminal offence to process personal data that is not registered (see Appendix 3).
	2. All staff are responsible for ensuring that:
		1. any personal data which they hold is kept securely
		2. personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party
		3. personal data is disposed of carefully either by shredding or identifying as confidential waste for disposal and collection by Premises staff (please refer to Appendix 5 for archiving guidelines)
	3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. The legislation provides for some actions relating to data protection to be a criminal offence.
	4. Personal information should be:
		1. kept in a locked filing cabinet; or
		2. in a locked drawer; or
		3. if it is computerised, be password protected; or
		4. kept only on an external storage device (eg memory stick) which is itself secure
		5. kept safe and secure (see Appendix 2)
	5. Where data is in use, or is moved from one storage place to another, additional care must be taken to prevent the data being used or disclosed inappropriately (see Appendix 2).
	6. Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:
		1. electronic devices such as laptops or PDAs and computer media (USB sticks, etc) that contain personal data are not left unattended
		2. all the security guidelines given in this document are followed
	7. Personal data should not be processed at staff members’ homes except in the case of high end data users where this may be permitted but only with the express agreement of the College’s Data Protection Officer or the Principal or Deputy Principal Corporate Resources in the absence of the Data Protection Officer. In such circumstances all the security guidelines given in this document must still be followed.
10. **Publication of College Information**
	1. Information that is already in the public domain is exempt from the 1998 Act. It is the College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:
		1. Names of College Corporation members and Register of Interests of Corporation members and staff with significant financial responsibilities (for inspection during office hours only via the Clerk to the Corporation)
		2. College and Faculty/Department organisational charts
		3. Information on examination results
	2. The College’s internal phone list will not be a “public document” although it is widely available.
	3. Any individual who believes that they have good reason for wishing details in these lists or categories to remain confidential should contact the Head of Human Resources.
11. **Processing Personal Data and Subject Consent**
	1. The College can only process personal data with the consent of the individual (see Appendix 1 – “Use of Personal Information and Consent Statement”). The information that staff deal with on a day-to-day basis will be ‘standard’ and will cover the categories listed under Appendix 3.
	2. If the data is ‘sensitive’ (see Appendix 1) express consent of the data subject must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. This includes information about previous criminal convictions.
	3. College staff and some students will come into contact with children, including young people up to 18 years old. The College has a duty under the Children Act (2004) and other enactments to ensure that staff are suitable for the job and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use College facilities do not pose a threat or danger to other users.
	4. The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.
	5. Therefore all prospective staff and students will be asked to sign a “Use of Personal Information and Consent Statement” (see Appendix 1) when an offer of employment or course offer is made. A refusal to sign such a form can result in the offer being withdrawn.
12. **References**
	1. It should be assumed that all written or computer stored data (including comments, notes and references) about any student or any member of staff could become disclosed to that person and therefore any comments made on individuals should be made with this in mind. In particular it should be assumed that all references could be disclosed to the individual about whom the reference is written. It should not be assumed that a reference headed “confidential” may not be disclosed to the subject of the reference.
13. **Retention and Disposal of Data**
	1. Appendix 5 outlines the College’s guidelines for archiving and the retention period for data. See 9.2 above and Appendix 2 relating to the disposal of data.
14. **Designated Points of Contact**
	1. The designated points of contact for enquirers relating to the Data Protection Act are:
		1. The College’s Data Protection Officer – Head of IT Services in Room 019 in the Forest Road Building.
		2. The Head of Human Resources in Room 311 in the Forest Road building.
15. **Review Arrangements**
	1. This version of the Policy was originally approved by the Principal on 31 October 2011 and minor amendments were made in December 2013 and December 2014. A further update was made in September 2017. The Policy is for immediate application and will be reviewed at least every 2 years by the Executive Team or when required by legislation or the needs of the College.

**Appendix 1**

**Definitions**

**Important definitions relating to the legislation and/or this Policy:**

* **Data** – Data can be in electronic or paper-based form and is any system that is a “structured set of personal data” and the records can be “centralised, decentralised or dispersed”. This means all our staff and student records.
* **Data Controller** – The Data Controller is the legal “entity” who determines the purposes of which data is collected. The College is the Data Controller.
* **Data Protection Officer** – The College’s Data Protection Officer is the Head of IT Services who is responsible for maintaining the College’s registration with the Information Commissioner’s Office and providing advice and guidance to assist in ensuring compliance with the Data Protection Act.
* **Data Subject** – Is the living individual who is the subject of the data. This will include staff, students, contractors, suppliers, visitors and anyone else about whom the College collects personal data.
* **Personal Data** – This is information that relates to an individual who can be identified from that information either by itself or when used in conjunction with other information in, or likely to come into, the possession of the Data Controller.
* **Processing data** means performing any operation or set of operations on data, including:
* Obtaining, recording or keeping the data
* Collecting, organising, storing, altering or adapting the data
* Retrieving, consulting or using the data
* Disclosing the data by transmitting, disseminating or otherwise making it available
* Aligning, combining, blocking, erasing or destroying the data
* **Sensitive Personal Data** relates to specific categories of data which are defined as data relating to a person’s racial origin, political opinions or religious or other beliefs; physical or mental health; sexual orientation; criminal convictions or the alleged commission of an offence; trade union membership.
* **Stored Data:**
* **Automated data** means any information on computer or information recorded with the intention of putting in on computer
* **Manual data** means information that is kept as part of a “relevant filing system” or with the intention that it should form part of a relevant filing system
* **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible
* **Use of Personal Information and Consent Statement** – This is included on the Student Enrolment Form and the Staff Job Application Form and normally on other documents used to collect data to indicate how any data provided will be processed by the College.
* **Third Party –** Is anybody other than the Data Subject, Data Controller or other person authorised to process personal data on behalf of the College.

#### Appendix 2

**Staff Guidelines on handling personal information**

**Do’s:**

|  |  |
| --- | --- |
| ✓ | **Consider the following checklist prior to processing any personal information**Do you really need to record the information?* Has the data subject been told and given consent to this type of data being processed?
* Are you authorised to collect/store/process the data?
 |
| ✓ | **Keep any personal information you are authorised to hold safe, secure, accurate and up-to-date:*** Keep your system password(s) secure and never share with others
* Hard copy personal information should not be left open on desks when you leave the room
* Computer screens should be positioned so that personal information is secure
* Electronic files should not be left open on computer screens when you leave the room. Use your password protected screensaver
* Store any personal data on areas of the College network where access is restricted, or on an external storage device (eg portable memory stick) which is securely locked away
* Rooms where personal files are kept should be locked when empty
* Filing cabinets, drawers or cupboards containing personal information should be locked when not in use
 |
|  |  |

**Don’ts:**

|  |  |
| --- | --- |
| 🗶 | Disclose any personal information to any unauthorised person at ***ANY*** time or for ***ANY*** reason |
| 🗶 | ***NEVER*** give out information concerning a student or member of staff over the telephone. Information ***in writing*** should only be given where you are authorised to provide it and the person you are giving it to is authorised to receive it  |
| 🗶 | ***NEVER*** give your Network or College systems password(s) to ***ANYONE*** for ***ANY*** reason |
| 🗶 | ***DO NOT*** destroy personal records without referring to the “Guidelines for Archiving” in Appendix 5 to this Policy and all papers and printouts should be disposed of carefully either by shredding or identifying as confidential waste for disposal |

**Categories of personal information held on staff and students**

#### Appendix 3

* **Personal details:** this includes date of birth; gender; ethnicity; name, address, telephone, mobile and email contacts; qualifications; next of kin; employment status.
* **Health or medical matters:** this includes details about specific conditions individuals may suffer from, such as asthma or diabetes: information about pregnancy, if appropriate, information about sickness absences and any medical reports we may have received.
* **Membership/non membership of trade unions**
* **Details about student academic performance** and expected results; attendance; individual learning plans; references and recommendations; records of any security or disciplinary issues; and any other course related information.
* **Details about student finance,** including course fees, course registration, library and other equipment on loan.
* **Details about employees work performance,** including notes of supervision sessions; appraisals; training and assessment; teaching and learning observation records, where appropriate.
* **Human Resources information.** This includes details about start date; pension and pay details; national insurance number, bank account details for pay purposes; next of kin; any current disciplinary or grievance matters; any deductions from salary or any loans.
* **Details about any criminal record**
* **Other categories** that may be relevant for the purposes of conducting the College’s legitimate business or requested by Government agencies from time to time.

#### WALTHAM FOREST COLLEGE

#### Appendix 4

#### DATA PROTECTION

#### STANDARD REQUEST FORM FOR ACCESS TO DATA

I, ***(insert name)*** wish to have access to either ***(delete as appropriate)***

1. All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that the College has about me in the following categories:

Personal details including name, address, date of birth, etc.

### Health or medical matters

Trade Union information

### Student academic performance

Student Finance

Academic or employment references

Employees work performance

Disciplinary records

Any statements of opinion about my abilities or performance

Other information: please list below

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Please tick as appropriate)

I understand that I will have to pay a fee of £10

(The College will make no charge for the first occasion that access is requested)

Signed

Dated

Students should return this form to - College Administration Office

Staff should return this form to - Human Resources Office

Other users - Reception

The form will then be forwarded to either the Head of HR or the Data Protection Officer.

#

# WALTHAM FOREST COLLEGE

**Appendix 5**

# DATA PROTECTION

# GUIDELINES FOR ARCHIVING

|  |  |  |
| --- | --- | --- |
| **Type of Data** | **Retention Period** | **Reason** |
| Human Resources Files; training records; notes of grievance and disciplinary hearings | 6 years from the end of employment.Grievance and disciplinary files will be kept separate from the main personal file but will also be kept for 6 years from the end of employment. Records of disciplinary warnings will only be kept for as long as specified in the Disciplinary Procedure. | Provision of references and limitation period for litigation |
| Safeguarding allegations against staff (excluding malicious allegations) | Records will be retained for at least until the accused has reached normal retirement or for a period of 10 years from the date of the allegation if that is longer. | Statutory Guidance for Schools and Colleges (April 2014) |
| Staff Application forms; interview notes | 6 months from the date of the interviews | Limitation period for litigation |
| Facts relating to redundancies (less than 20) | 3 years from the date of redundancies | Limitation period for litigation |
| Facts relating to redundancies (20 or more) | 12 years from the date of redundancies | Limitation period for litigation |
| Income Tax and NI returns; correspondence with Tax Office | 3 years after the end of the financial year to which the records relate | Income Tax (Employment) Regulations 1993 |
| Statutory Maternity Pay records and calculations | 3 years after the end of the financial year to which the records relate | Statutory Maternity Pay (General) Regulations 1986 |
| Statutory Sick Pay records and calculations  | 3 years after the end of the financial year to which the records relate | Statutory Sick Pay (General) Regulations 1982 |
| Wages and salary records | 6 years from the last date of employment | Taxes Management Act 1970 |
| Records and reports of accidents | 3 years after the date of the last entry | RIDDOR 1985 |
| Health Records | During Employment | Management of Health and Safety at Work Regulations |
| Health Records where reason for termination of employment is concerned with health, including stress related illness | 3 years | Limitation period for personal injury claims |
| Medical Records kept by reason of the Control of Substances hazardous to health | 40 years | COSHHR 1994 |
| Student Records including academic achievements, and conduct | 6 years from the last day of the course10 years with the consent of the student for personal and academic references | Limitation period for negligence |
| To 31 December 2022 | European Social Fund (ESF) requirement |