11.6 Confidentiality and Data Protection procedure

Issue date: December 2013

Review date: July 2015

Introduction

The purpose of this procedure is to set out the way in which confidential information and data should be protected, handled and transferred within the organisation

Aims and objectives of the procedure

This procedure sets out the School`s formal arrangements for safeguarding confidential information and data and also provides definitions and guidance. It forms one of a series relating to the Human Resources Policy (11).

Defined responsibilities

Operational responsibility for this procedure lies with the Human Resources Manager and the College Registrar. However, all staff have responsibility for ensuring that confidential student information is protected.

Operational description

This procedure has the following sections:

1. Confidentiality
2. Data Protection
3. Definitions
4. Purposes of obtaining data
5. Collection and use of personal data
6. Physical security of personal data
7. IT security
8. Surveillance
9. Compromised data
10. Third Party Data Processors
11. Tight to access information
12. Disclosing information to the Police
13. Confidential waste

There are two annexes:

11.6.1 Confidentiality Agreement (employees)
11.6.2 Data Processing Agreement (Data Processors)

1 Confidentiality

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It:

- is a legal obligation that is derived from case law
- is a requirement established within professional codes of conduct
- must be included within EThames Graduate School employment contracts as a specific requirement linked to disciplinary procedures

Information should be considered confidential if it can be related in any way to a specific individual. Confidential information will be found in a variety of formats including paper, electronic (including portable devices such as laptops, palmtops, smartphones, CDs, DVDs), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone (including mobiles) and general conversation.

1.1 Limits of confidentiality

The college will respect a student's wish for confidentiality except in situations of perceived risk of significant harm to the student or others. This includes safeguarding concerns and the risk of serious crime being committed. For this reason, it is important that you **never offer absolute confidentiality** and that the limits to confidentiality are explained.

2 Data Protection

This Procedure outlines EThames Graduate School's ('the Company`s') commitment to the Data Protection Act 1998 ('the Act') and provides a framework for the School's compliance with and implementation of the Act.

EThames Graduate School collects and uses information about individuals, including students, information on members of the public, customers, suppliers, employees (past and current) and all others with whom the School communicates.

In handling personal data, the School is required by law to fulfil certain statutory duties and, in particular, to comply with the terms of the Data Protection Act 1998 ('the Act'). The Act establishes a framework of rights and duties which are designed to safeguard personal data. EThames Graduate School fully endorses the statements and intent of the Data Protection Act and recognises that it must treat personal information correctly and lawfully. The School regards compliance with the Act as essential to creating and maintaining confidence between the School and individuals with whom the School communicates.

EThames Graduate School will implement these procedures to ensure that all employees (both administrative and academic), self-employed workers and contractors, agents, consultants or other partners of the School who have access to personal data held by or on behalf of EThames Graduate School are fully aware of and adhere to the responsibilities and duties established by the Data Protection Act.

2.1 Data Protection principles

The Data Protection Act 1998 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature. It is founded on the following set of eight good practice principles:

- **Principle 1** – Personal data shall be processed fairly and lawfully and in particular shall not be processed unless specified conditions can be met
- **Principle 2** – 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
- **Principle 3** – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- **Principle 4** – Personal data shall be adequate and where necessary kept up to date
- **Principle 5** – Personal data processed for any purpose or purposes shall not be kept any longer than is necessary for that purpose or those purposes
- **Principle 6** – Personal data shall be processed in accordance with the rights of data subjects
- **Principle 7** – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful: processing of personal data and against accidental loss or destruction of or damage to personal data
- **Principle 8** – Personal data shall not be transferred to any country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

2.2 Management of personal data

Where EThames Graduate School takes any decision which significantly affects any member of staff or student exclusively upon the results of an analysis of his/her personal data carried out by automated means then we will provide that person with notice of this fact as soon as reasonably practicable thereafter. If the decision is connected with a contract entered into between the School and another person or is taken for the purposes of considering whether to enter into or with a view to entering into such a contract, the other person will be allowed to make representations on the outcome of that decision (perhaps as part of a formal grievance procedure).

In the event of a potential intended or actual transfer of a business, the School will take all reasonable steps to limit disclosure of personal data about employees to any of the third parties concerned by for instance, the omission of names or other identifying particulars. However, staff should be aware that some personal data such as name, address, position, salary levels may be transferred to a prospective operator (or other similar party) of any part of School operations as part of a due diligence process.

Where this happens the School will place contractual obligations on the prospective operator to keep the member of staff's information safe. The transferee shall cease to be a third party on the date of the formal transfer, except in respect of the personal data concerning certain rights and obligations such as those relating to supplementary pensions – not required under the Transfer of Undertakings (Protection of Employment) Regulations 1981 as amended by the Trade Union Reform and Employment Rights Act 1993.

2.3 Information Commissioner's Office

Information Commissioner's Office (ICO) is the UK's independent authority, set up to uphold information rights in the public interest and data privacy for individuals.

EThames Graduate School is registered with the ICO as a 'data controller' for the purposes of the Data Protection Act 1998. This registration provides the Information Commissioner's Office with details about the purposes for which the School processes personal information and the types of personal data collected. The registration is renewed annually in September and will review and update it as required.

2.4 Responsibilities

All individuals should take personal responsibility for ensuring that personal data that they collect and process is done so in accordance with the Data Protection Act 1998 and in accordance with this procedure. All due care and attention should be taken to ensure that the privacy of the data subject is maintained; this must be treated as a matter of priority.

It is the responsibility of all line managers to ensure that this procedure is followed. They should ensure team members have read and agreed to abide by the procedure and are aware of the Data Protection Act 1998

The School expects all students and staff to use computers, email and the Internet responsibly and in accordance with the data protection principles. They should also make themselves aware of the provisions contained in Procedure 11.20 on IT and internet use.

Students and staff are expected to adhere to this procedure and to ensure that those for whom they are responsible both adhere to this policy and protect computer systems and personal data from security risks. Where necessary, managers should seek advice from the IT Department to assist in these goals.

Formal responsibility for ensuring that staff and operational procedures comply with the Data Protection Policy and Procedure lies with directors, managers, team leaders or supervisors in each operational area of the School.

Staff must become familiar with the aims of this procedure and follow the guidelines set out. In particular staff should:

- seek advice from their line supervisor, team leader, manager or director or the Director of Information Management where they have an doubts as to whether or not the processing of personal data that they require to carry out in the course of their employment complies with the Act
- not use personal information that they hold in the course of their employment for any reason other than the performance of their employment duties. (To procure personal information from the School and use it without its consent is likely to constitute a criminal offence under the Act)
- provide all assistance to the Director of Information Management in the conduct of any audit or preparing a response to a subject access request
- keep information that they process for the School safe and secure in accordance with any procedures issued by the School. Where no procedures are set out explicitly, they should exercise a degree of care over the personal data that they process by considering the harm that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Director of Information Management

- not keep duplicate records relating to staff or students where a centralised filing option is available. Keeping personal records unnecessarily can complicate the process of responding to subject access requests
- notify the Director of Information Management immediately should you detect any potential or actual breach of the Act.

It is important that personal data held is accurate. All members of staff are required to inform the School if they believe that personal data is inaccurate or untrue or if they are dissatisfied with the information in any way.

2.5 Employee awareness and training

Employees at all levels need to be aware of what their roles and responsibilities are. Managers should take steps to train their staff to recognise threats such as phishing emails and other malware.

Training needs should be identified and training arranged as necessary. This responsibility extends to ensuring the importance of protecting personal data is prioritised in partnership working and data sharing arrangements. Should it be necessary to share information with other organisations under the provisions of Section 29 of the Act, the necessary forms should be completed and safeguards put in place to protect the data.

3 Definitions

Some helpful definitions are set out below to assist in the understanding of this procedure:

3.1 Confidential information

A duty of confidence arises when one body discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. In the context of this policy, confidential information can be:

- personal or sensitive information supplied on this basis to the School by an individual member of staff
- information supplied under contractual arrangement from another body or organisation

3.2 Personal data

This means data (manual or electronic) which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of or is likely to come into the possession of the Data Controller. It also includes any expression of opinion about an individual and any intentions of the data controller or any other person in respect of the individual. Personal data must be processed fairly and lawfully and, in particular, shall not be processed unless one of the Conditions set down in Schedule 2 of the Data Protection Act 1998 is met.

3.3 Data

This means any information that is being processed automatically or is recorded with the intention of being processed automatically. Any data recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system is also included in this definition.

3.4 The Data Controller

This means a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed. For the purpose of this procedure, EThames Graduate School is taken to be the Data Controller.

3.5 The Data Subject

This means the individual who is the subject of the personal data.

3.6 Processing

This means obtaining, recording or holding the information or carrying out any operation on the data; including organisation, adaptation or alteration of the information or data; the retrieval, consultation or use of the data; the disclosure of the data and the alignment, combination, blocking, erasure or destruction of the information or data. It is difficult to imagine any activity which does not amount to processing.

3.7 Sensitive personal data

This means personal data consisting of information as to an individual's racial or ethnic origin, political opinions, religious or other beliefs; physical or mental health or condition; sexual orientation; the commission or alleged commission of an offence or any proceedings for any offence committed or alleged to have been committed by an individual.

The presumption in respect of sensitive personal data is that because information about these matters is likely to be of a particularly sensitive nature it needs to be treated with greater care than other personal data. This is particularly so as the loss, theft or mishandling of this category of information is likely to be of a greater detriment to the individual than the loss, theft, etc., of other categories of personal data.

Sensitive personal data must be processed fairly and lawfully and shall not be processed unless one of the Conditions set down in both Schedule 2 and Schedule 3 of the Data Protection Act 1998 are satisfied. The nature of the data is also a factor in deciding what security measures are necessary to protect the information.

4 Purposes of obtaining data

In order to fulfil individuals' contracts of employment, monitor sickness and performance, equal opportunity policies and otherwise administer the School's business, we will use and process personal information relating to employees which we have obtained during the course of their employment. Such information includes:

- Employment history
- Personal circumstances
- Educational qualifications
- Sickness records
- Medical records
- Accident reports.
- Incident records
- Attendance record

- Convictions
- Performance reviews
- Disciplinary records
- Ethnic or racial origins
- Salaries

EThames Graduate School holds personal data about employees confidentially and will only disclose it to others where there is a need to do so; eg. to give information about earnings to HM Revenue & Customs. No sensitive data such as information about an individual's health, racial or ethnic origins, sexual orientation, criminal convictions, political affiliation or religious belief will be divulged to a third party without the individual's permission, unless there is a specific legal requirement to process such data.

5 The collection and use of personal data

EThames Graduate School collects and uses personal information (names, addresses etc) in many ways and therefore must meet its legal obligations under the Data Protection Act 1998. In particular:

- the School shall only collect and use personal data where it has legitimate reasons for doing so
- when personal data is collected it should be for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose (the Second Data Protection principle)
- the personal data collected should be adequate, relevant and not excessive for the purpose for which it is processed (the Third Data Protection principle)
- when personal data is obtained it shall be processed fairly and lawfully (the First Data Protection principle) and should be accurate and, where necessary, kept up to date (the Fourth Data Protection principle)

6 Physical security of personal data

There is an obligation under the Data Protection Act for the School to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data (the Seventh Data Protection principle). Some technical security measures are set out below and should be adhered to. This is not an exhaustive list and anyone handling personal data on behalf of the School must take all steps necessary to protect personal data and keep it secure at all times.

Physical security measures should be in place to protect personal data. This includes things like locking doors, securing filing cabinets containing personal information, protecting premises with alarms, security lighting and CCTV cameras.

It also includes ensuring that access to School premises is controlled and monitored. The School has a Visitor Book for all staff and non-staff members entering the campus (in reception area) requiring visitors to sign in and out of the premises. They must also state the time of their arrival and departure from the premises. All visitors to School will be provided with visitor passes on arrival.

6.1 Manually held personal data

Each Department must ensure that it knows and holds a record of what personal data it holds and how and where it is stored.

6.2 Paper files

The Date Protection Act only applies to personal information held on paper records where the paper record is structured by reference to an individual (or by reference to criteria relating to an individual) such that specific information about a particular person is readily accessible. That means that most filing systems will contain personal data. It is only very disorganised filing systems which may fall outside the scope of the Act.

It should be assumed, as a general rule, that personnel files and separate files relating to such criteria as disciplinary warnings or appraisals are covered by this Act. However, when in receipt of a subject access request, the School will assess whether or not the information in any particular file is information to which the Act applies before making any disclosure.

6.3 The processing of manually held personal data by fax or post

When information containing personal data is sent by fax extra care should be taken. For example fax numbers should be checked to ensure that the information is being sent to the correct recipient. In addition you should ring ahead to the recipient and advise them that the information is being sent. You should also ask the recipient to acknowledge receipt of the information. Sensitive personal data should only be faxed as a last resort.

When confidential and sensitive personal data are being sent via post the information should be checked by another member of staff before being sent to ensure it is being posted to the correct recipient. In addition staff should 'double bag' information being sent where the information contains sensitive personal data or personal data of a confidential nature. Double bagging works by putting the personal data in an inner envelope which marks the material as confidential and has a postal return address. The inner envelope acts as a second barrier to the information being opened by the wrong recipient accidentally or otherwise.

All personal data sent to printers should be collected immediately and either stored securely or disposed appropriately. Personal data should not be left on printers, photocopiers, fax machines, etc.

6.4 Clear desk arrangements

As a general rule personal data should never be left unattended on desks or in meeting rooms etc. Further and upon the implementation of the Data Protection procedures the School should operate a clear desk arrangement. This reduces the risk of unauthorised access to, loss of or damage to personal data. It will also ensure that all personal data and confidential information held by the School is held securely and adequately protected.

The clear desk arrangement means that at the end of each day it is the responsibility of individual employees to clear their desk of all documents that contain any personal data or confidential information. This information must be stored safely and securely (for example, in a locked office, locked filing room or filing cabinet).

7 IT security

Personal data held on computers and computer systems (including any information held on back-up systems) must be protected by the use of secure passwords. Individual passwords should not be such that they can be easily compromised.

Computers must not be accessible when unattended. All staff is responsible for safeguarding data by ensuring that equipment is not left logged-on when unattended. Staff leaving their computer station for short periods should always 'lock' their computer. This is done by pressing the 'Ctrl, Alt and Delete Keys' (simultaneously); and then choosing the 'Lock Computer' option. To unlock their computer staff should enter their log-in details.

7.1 Physical security

To ensure that equipment containing personal data is not easily stolen during a break-in, EThames Graduate School servers are stored in a secure communications room with added protection. Backup servers are also stored in the communications rooms

7.2 Anti-Virus and Anti-Malware

EThames Graduate School uses **MS System Centre Frontline Protection** which is an anti-virus and anti-malware software which scans the network to prevent and detect threats. The schools servers are managed by an third party 'Control Esc' who maintain and daily monitor the network for threats. Control Esc also makes sure MS System Centre Frontline Protection is kept up-to-date.

7.3 Intrusion defence

EThames Graduate School is able to stop breaches happening before they penetrate deep into the network, by installing **Draytek Firewall** on the network and **Windows Personal Firewall** on each PC used within the School.

7.4 Access controls

Each user has their own username and password to access the network, access Outlook and access SIS database. Each new member of staff is informed during induction never to share their username and password with others.

A brute force password attack is a common method of attack. It is simplest kind of method to gain access to a site by trying usernames and passwords, over and over again, until it gets in. Often deemed 'inelegant', they can be very successful when people use passwords like '123456' and usernames like 'admin.' They are, in short, an attack on the weakest link in any website's security. To prevent a brute force attempt each user is allocated **five attempts** to correct enter their username and password. Also, the student network has no access to the servers VLAN therefore it is not possible for a student hack the school main network. Students and staff WI-FI is different and the staff WI-FI SSID is hidden from view from any non-staff device.

Passwords or other accesses are cancelled immediately a staff member leaves the organisation or is absent for long periods. The HR department raises a helpdesk ticket whenever a user account needs to be cancelled or suspended.

7.5 Segmentation

To prevent or limit the severity of data breaches EThames Graduate School separates and limits access within different components for the Virtual Local Area Network (VLAN). This means that if one area is compromised, the attacker would not have direct access to other data stores.

7.6 Device hardening

EThames Graduate School's IT department is currently working towards having a **software inventory**. This inventory will help pinpoint which software needs to be removed, updates required and possible security vulnerabilities. Older versions of some widespread software have well documented security vulnerabilities. If software is not being used the IT Department will remove rather than try to keeping it up-to-date. The IT department always changed default passwords used by software or hardware, as these are well known by attackers.

7.7 Sending personal data by email or any other electronic media

Anyone sending personal data via email or electronic media must ensure that it is encrypted. Passwords protecting the information should also be used depending on the sensitivity of the personal data. Passwords must never be emailed. The sender should contact the recipient via telephone to provide the password to decrypt the data.

When emailing personal data extra care should be taken that the information is being sent to the correct recipient and is adequately protected. Email addresses should always be checked prior to information being sent via email to ensure the content is being sent to the correct recipient.

7.8 The use of removable media devices

EThames Graduate School will ensure the controlled use of removable media devices used to store and transfer information for the purpose of conducting official business. Removable media includes laptops, mobile phones, tablets, CDs, DVDs, Optical Disks, External Hard Drives, USB Memory Sticks; media card readers, microchips (including SIM Cards), MP3 Players and digital cameras. The following guidelines must be adhered to when using approved removable media devices:

- all removable media devices and associated equipment must only be purchased and installed by the IT Department
- non-School owned removable media **must not** be used to store any information used to conduct official School business and must not be used with any School owned equipment, unless any have been authorised by a senior manager
- only data that is authorised and necessary to be transferred should be saved on removable media devices
- removable media must not be used for archiving or storing records
- anyone using removable media devices must be responsible for them and must take all steps necessary to protect the device and data from loss, theft or damage
- removable media should not be the only place where personal data held for School purposes is held. This increases the risk of the loss, destruction or malfunction of the data. Copies of the information should be held on the School's computer system
- in order to minimise physical risk, loss or theft or electrical corruption all storage media must be

stored in an appropriately secure and safe environment

- each user is responsible for the appropriate use and storage of the data and for not allowing any removable device to be comprised
- each laptop and mobile device should have a unique password
- all software and data stored on removable media devices must be encrypted and / or password protected (depending on the sensitivity of the data)
- damaged or faulty removable media devices must not be used
- virus and threat management software approved by the IT Department must be used to scan removable media devices as soon as they are connected to School IT equipment
- where removable media devices are no longer required or are damaged etc they must be disposed of securely to avoid data leakage. Any previous content must be permanently erased. All removable media devices that are no longer required /damaged etc must be returned to the IT Department for secure disposal. For advice on removing all data (including deleted files) from removable media please contact the IT Department
- if any School mobile / removable media device is lost, stolen or otherwise compromised you must report this immediately to the IT Manager and HR Manager.

7.9 Home working and removal of personal data from School premises

As a general rule, manual and electronic records containing personal data should not be removed from the School premises. Further, records containing personal data should never be left unattended and the appropriate measures should be taken to ensure that it is not left in public places, on public transport or in cars etc.

Personal data processed on behalf of EThames Graduate School should not be held by staff at their homes, whether paper documents or digital data stored on a device, or a staff members personal computer/laptop or hard drive.

However, there will be occasions where some staff may be authorised by senior management to work from home. When dealing with personal information at home or outside of EThames Graduate School premises the same measures must be applied as if working in the office. Staff must ensure that the appropriate technical and organisational measures against the unauthorised or unlawful processing of the personal data and against the accidental loss or destruction of, or damage to, personal data.

Members of staff that are home working, are responsible for the security of equipment, software, files and any other information in their possession outside of the School premises. All paperwork held outside of the School's premises should be securely locked away (when not in use). It is particularly important to ensure that non-authorised personnel (in the home environment or whilst working off site) cannot gain access to confidential or personal information. Considerations should be made when working remotely on laptops to ensure that the screen cannot be overseen by others and precautions taken to avoid laptops and other mobile devices being stolen or lost.

8 Surveillance

The School has a legitimate interest in monitoring the behaviour of its staff and students. For instance, the School may wish to carry out monitoring in order to:

- detect harassment or other inappropriate behaviour

- monitor performance of its staff or of students where this is appropriate
- monitor and detect the outward transmission of confidential information
- prevent and detect theft of School property
- prevent or detect any unlawful act
- monitor adherence to this and other policies
- perform other duties in the employment or education sphere.

Monitoring can take several forms. It can involve monitoring by way of Closed Circuit Television (CCTV), e-mail and Internet monitoring or telephone monitoring.

The School holds information on the destination and duration of calls made from its telephone system and may use this information if misuse of the system is suspected.

8.1 CCTV camera use

The School procedure for the use of CCTV cameras is as follows:

In carrying out monitoring the School may use CCTV cameras in what are considered to be 'public' areas of the workplace. Generally, the use of such CCTV cameras shall be notified by using suitable signage at obvious places at the entrance to the monitored areas, however, (even in the absence of such signage) students and staff should be aware that public space within School premises may be monitored in this way. The School has notified such monitoring to the Information Commissioner and will use the footage in disciplinary or other proceedings where appropriate.

The School may also monitor through the use of covert CCTV but it shall only do so where specific criminal activity has been identified. Before starting any use of covert CCTV the School will have made an impact assessment concluding that notifying staff of the use of such covert monitoring would prejudice the investigation and that the use of covert monitoring techniques is a proportionate response to the behaviour in question. Where appropriate, (but at its absolute discretion) the School will involve the police in such monitoring.

9 Compromised data

Information security breaches may cause real harm and distress to the individuals they affect; lives may even be put at risk. Examples of the harm caused by the loss or abuse of personal data (sometimes linked to identity fraud) include:

- fake credit card transactions
- witnesses at risk of physical harm or intimidation
- offenders at risk from vigilantes
- exposure of the addresses of service personnel, police and prison officers, and women at risk of domestic violence
- fake applications for tax credits
- mortgage fraud

9.1 Action to be taken if data goes missing

The Head of Department must be informed immediately if any confidential or sensitive data goes missing. An immediate investigation will be launched to discover where the data has gone.

If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data. If that individual has, and the data was correctly encrypted, compressed and password protected it suggests that the individual has unlawfully accessed the data. In such situations it might be appropriate to involve the police in the investigation.

The Head of Department will consider whether any individuals need to be informed about the data having gone missing, even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person.

9.2 Negligent transfer of data

If an employee has been negligent in transferring sensitive and confidential data this might be considered to be gross misconduct, which might result in summary dismissal. This is particularly likely to be the decision if:

- the employee did not encrypt, compress and password protect data
- the employee transferred data using the open post and did not use a courier service
- the employee transferred data without seeking the appropriate approvals.

10 Third Party Data Processors

This section applies to third party external organisations, companies and individuals (other than employees) who process personal information on behalf of EThames Graduate School. Third parties holding or processing personal data on behalf of the EThames Graduate School are known as 'Data Processors.' When the School contracts or arranges for someone to process personal data on its behalf the School remains responsible for the processing and is liable for any breaches of the Data Protection legislation caused as a result of that processing.

Therefore, when EThames Graduate School engages another organisation to process personal information on its behalf the School must make sure that the Data Processor only uses and discloses the personal data in accordance with EThames Graduate School instructions and must require the Data Processor to take appropriate security measures.

In light of the above all Data Processors are required to confirm that they are willing and able to abide with the requirements of the Data Protection Act 1998 and the EThames Graduate School's Data Protection procedures.

10.1 Data processing agreement

All Data Processors will be required to sign a Data processing agreement (see 11.6.2)with EThames Graduate School confirming their commitment to process personal data on behalf of EThames Graduate School in accordance with the Data Protection legislation. This is an agreement that sets out the terms and conditions under which personal data held by the specified 'data controller' will be processed by the specified 'data

processor'. This agreement is entered into with the purpose of ensuring compliance with the Data Protection Act 1998. Any processing of data must comply with the provisions of this Act.

10.2 Engaging Data Processors

The items listed below are further good practice recommendations that must be followed when engaging data processors:

- engage a reputable company which offers suitable guarantees to ensure the security of personal data. Guarantees provided by a company must be of a similar standard to the protection afforded personal data under EThames Graduate School Data Protection procedure.
- make sure that the organisation has appropriate security measures in place
- check if the organisation is registered with the Information Commissioner's Office
- require the organisation to report any security breaches or other problems

The selected organisation will be required to indemnify the School against any prosecutions, claims, proceedings, actions or payments of compensation or damages arising as a result of a breach of the Data Protection Act without limitation.

10.3 Overseas transfer of data

The Act forbids transfers of personal data to recipients in countries outside the EU, including transfers in machine-readable forms such as tapes or discs, unless specific conditions are complied with. You must not therefore transmit or carry personal data to countries outside the UK without first satisfying yourself that the transfer is permitted. You are required to refer to you're the senior managers in these circumstances before any transfer is made.

11 Right to access information

Under current legislation, individuals are entitled to have access to certain personal data held about employees. If an employee requires access, they should contact their line manager. The request should be made in writing specifying the information required.

All requests for details on personal data must be made in writing and with a £10 fee. In response, EThames Graduate School will provide copies of the information held. Please note that there may be circumstances where information cannot be provided because doing so would involve disclosing information on others and it is reasonable to withhold information for these reasons.

Requests from employees will be handled by Human Resources. All requests will be dealt with within a reasonable timescale, but no longer than 40 days.

12 Disclosing information to the Police

The School is committed to acting in a lawful and ethical manner and expects its students to act similarly. Where the Police advise the School that they wish to receive information in respect of a student they believe has committed an offence, the School will provide them with the following personal information:

- personal details (name, address, contact number)
- course details (course of study and mode of attendance)
- current status details (whether a student is active or withdrawn)

Timetable/rooming information will not be provided.

The School will offer to contact the student direct and request that they speak to the police. If the student so wishes, the student may ask to be accompanied by a member of staff if the meeting takes place on School premises during normal working hours.

The police must provide an information request form (under the Data Protection Act 1998 section 29(3)) in respect of all enquiries.

13 Confidential waste

Student Services, Marketing and Human Resources departmental records contain confidential information on employees. Therefore, procedures should be in place to ensure that information is disposed of correctly.

13.1 What is classified as confidential waste?

Confidential waste is regarded as any documentation that shows employee personal details, post details or salary details; any information which is personal and identifiable to an individual.

13.2 Storage of confidential waste

All confidential waste will be stored in secure areas accessible only to authorised personnel.

13.3 Responsibility for disposal of confidential waste

Within each department a designated individual should be responsible for the safe disposal of confidential waste at regular intervals.

Any member of staff employed by the School must ensure that they comply with the procedure for sealing with confidential waste at all times. Failure to comply with any part of this procedure could result in disciplinary action being taken, up to and including dismissal.

11.6.1

.

CONFIDENTIALITY AGREEMENT

THIS AGREEMENT is made the _____ day of _____ year _____
BETWEEN:

(1) EThames Graduate School (the Company); and
(2) _____ (the Employee).

WHEREAS:

(A) The Company agrees to give the Employee access to certain confidential information relating to the affairs of the Company solely for purposes of:
_____
_____
_____
_____

(B) The Employee agrees to obtain, inspect and use such information only for the purposes described above and otherwise to hold such information confidential and secret pursuant to the terms of this agreement.

NOW IT IS HEREBY AGREED as follows:

1. The Company has or shall furnish to the Employee confidential information, described on the attached list, and may further allow suppliers, customers, employees or representatives of the Company to disclose information to the Employee.
2. The Employee agrees to hold all confidential or proprietary information or trade secrets ("Information") in trust and confidence and agrees that the Information shall be used only for the contemplated purpose, and not for any other purpose or disclosed to any third party under any circumstances whatsoever.
3. No copies made be made or retained of the Information.
4. At the conclusion of our discussions, or upon demand by the Company, all Information, including written notes, photographs, or memoranda shall be promptly returned to the Company. The Employee shall retain no copies or written documentation relating hereto.
5. This Information shall not be disclosed to any employee, consultant or third party unless that third party agrees to execute and be bound by the terms of this agreement, and disclosure by the Company is first approved.
6. It is understood that the Employee shall have no obligation with respect to any information known by the Employee, or as may be generally known within the industry, prior to date of this agreement, or that shall become common knowledge within the industry thereafter.
7. The Employee acknowledges the Information disclosed herein contains proprietary or trade secrets and in the event of any breach, the Company shall be entitled to apply for injunctive relief and to claim for damages of breach.
8. This agreement shall be binding upon and inure to the benefit of the parties, their successors and assigns.
9. This constitutes the entire agreement.

IN WITNESS OF WHICH the parties have signed this agreement the day and year first above written

Signed for and on behalf of the Company

_____

Signed by or on behalf of the Employee

_____

In the presence of (witness)

11.6.2

Data Processing Agreement Template

DATA PROCESSING AGREEMENT

Between

EThames Graduate School
and
[*Name of Data Processor*]

This Agreement is made on the……day of…… in the year …….

BETWEEN:

(1) EThames Graduate School, which is located at 412 – 416 Eastern Avenue, Ilford, Essex, IG2 6NQ the "Data Controller"

AND

(2) [*Name of data processor and company number*], having its registered office at [*address of data processor*] (the "Data Processor").

1. Purpose

1.1 The processing by the Data Processor is for the purpose of: [*Insert purpose(s) here*] (the 'Purpose')

1.2 This process is consistent with the Data Controller's obligations under the Data Protection Act 1998.

2. Information Provision

2.1 The data controller agrees to provide the data processor with the relevant data required for 'the Purpose'.

2.2 The data processing required for 'the Purpose' will be conducted in accordance with the following conditions as required by the Data Protection Act 1998 s.33:

- Personal data will not be processed to support measures or decisions with respect to particular individuals.
- Personal data will not be processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.
- Where data contains personal data relating to vulnerable adults or persons under 18 years of age the Data Processor agrees to abide by the conditions of the Child Protection Act and additionally ensure those processing the data have a valid 'Criminal Records Bureau' check.

2.3 The information to be provided is as follows:

- [*Insert description of information provided*]

3. Use, Disclosure and Publication

3.1 The Data will be used solely for 'the Purpose'.

3.2 The Data Processor is to act only on instructions from the data controller.

3.3 The data shall not at any time be copied, broadcast or disseminated to any other third parties, except in accordance with this Agreement.

3.3 The data will not be disclosed to any third party without the written authority of the Data Controller.

3.4 The only exceptions to clauses 3.2 and 3.3 above will be where any person is required to give evidence in legal proceedings.

3.5 No steps will be taken to contact any party identified in the data unless an individual has given prior consent to this use and disclosure.

3.6 [*Optional: only required if the data is to be used for research purposes as defined in the Act*] The data will be depersonalised so that no personal identifiers will be present in any results, or will be retained by the data processor beyond the period of the research. Personal data will *only* be processed with a view to producing depersonalised information/results.

3.7 All personal data held by the data processor including any archive or back-up copies, will be returned to the data controller/destroyed [*Delete as appropriate*] at a date to be agreed by the relevant parties. After this date, the data processor must provide a written declaration confirming that the data has been destroyed/returned [*Delete as appropriate*].

3.8 The data processor will process data purely for the Purpose and will not retain or process data for any other purposes.

3.9 On reasonable notice, periodic checks may be conducted by an authorised employee of the University of East Anglia to confirm compliance with this Agreement.

4. Confidentiality

4.1 The parties shall not use or divulge or communicate to any person (other than those whose need to know the same for the Purpose, or without the prior written authority of the Data Controller) any Personal Data obtained from the Data Controller, which it shall treat as private and confidential and safeguard accordingly.

4.2 For the avoidance of doubt, the obligations of confidentiality imposed on the parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

4.3 The Data Processor will respect for the privacy of individuals in any part of the Purpose requiring the use of personal data.

4.4 The Data Processor will take no steps to attempt to identify any person from the Data or aggregate data by any data matching or other exercise except where required by the Purpose.

5. Security

5.1 The Data Processor agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the Data Protection Act 1998 to the Data, which states that: "appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In particular, the Data Processor shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing, transmission or transport
- deter deliberate compromise or opportunist attack, and

- promote discretion in order to avoid unauthorised access.

5.2 The Data Processor shall ensure that security measures, commensurate with those operated by the Data Controller, shall be in force and applied at all times.

5.3 Data will be delivered to the Data Processor using the following procedures:

- Entry will be by authorised personnel only. Data will be checked to ensure it is accurate and complete and compliant with the regulatory or partner body requirements.
- EThames Graduate School staff will extract the required data into an encrypted file, using a mutually-agreed encryption format. The data will be transmitted to the Data Processor via an encrypted USB stick.
- On completion of the task, the Data Processor will return the encrypted USB stick to EThames Graduate School.
- At no point must the data be placed on any other removable media such as a Compact Disk, or be placed on local computer storage such as a Laptop Hard Drive.

5.4 The Data Controller reserves the right to undertake a review of security provided by the Data Processor and may request access to the Data Processor premises for this purpose. Failure to provide sufficient guarantees in respect of adequate security measures will likely result in the termination of the contract.

5.5 The Data Processor will store the data securely whilst it is being processed and when it is not in use. This refers to the Data in both electronic and paper formats and to any discs, CD Roms, or tapes containing the data.

5.6 The Data Processor undertakes not to use the services of any sub-contractors in connection with the processing of the data without the prior written approval of the Data Controller.

5.7 Any security incidents, breaches and newly-identified vulnerabilities must be reported to the Data Controller by the Data Controller at the earliest opportunity.

6. Indemnity

6.1 In consideration of the provision of the Data for the Purpose the Data Processor undertakes to indemnify any of the persons or any authority referred to in paragraph 6.2 below against any liability, which may be incurred by such person or authority as a result of the Data Processor's breach of this Agreement.

Provided that this indemnity shall not apply:

- where the liability arises from information supplied which is shown to have been incomplete or incorrect, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on his part or on the part of any other person or authority referred to in paragraph 6.2 below;
- unless the person or authority claiming the benefit of this indemnity notifies the Data Processor as soon as possible of any action, claim or demand to which this indemnity applies, commits the Data Processor to deal with the action, claim or demand by settlement or otherwise and renders the Data Processor all reasonable assistance in so dealing;
- to the extent that the person or authority claiming the benefit of this indemnity makes any admission which may be prejudicial to the defence of the action, claim or demand.

6.2. Persons who may claim the benefit of this indemnity are as follows: any current or former employee of the University of East Anglia.

7. Disputes

7.1 In the event of any dispute or difference arising between the parties out of this Agreement, the parties will meet in an effort to resolve the dispute or difference in good faith.

7.2 This Agreement is subject to English Law and the jurisdiction of the English Courts. The parties will, with the help of a Centre for Dispute resolution, seek to resolve disputes between them by alternative dispute resolution. If the parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the parties shall be at liberty to commence litigation.

8. Termination and Variation

8.1 This Agreement will terminate at the completion of the Purpose.

8.2 The Data Controller may at any time by notice in writing terminate this Agreement forthwith if the Data Processor is in breach of any material obligation under this Agreement.

8.3 In the event that any party wishes to exit from this Agreement, that party shall serve a notice, in writing, to the offices of the other party of a date not less than 30 days from the date of the said notice, on which the party proposed to exit the Agreement.

8.4 In the event that either party wishes to vary any term of this Agreement that party will give notice, in writing to the offices of the other party, explaining the effect of and reason for the proposed variation. The parties shall within 30 days of receipt of such a notice meet to discuss the variation.

8.5 As the data controller of the personal data this Agreement covers, the Data Controller will have the final decision on any proposed variation to this Agreement.

9. Relationship between the Parties

9.1 The Data Processor shall give reasonable assistance as is necessary to the Data Controller in order to enable him to:

- Comply with request for subject access from the data subjects;
- Respond to Information Notices served upon him by the Information Commissioner;
- Respond to complaints from data subjects;
- Investigate any breach or alleged breach of the Act.

in accordance with his statutory obligations under the Data Protection Act 1998.

9.2 The receipt by the Data Processor of any Subject Access Request to the Data covered by this Agreement must be reported at the earliest opportunity to the Information Policy and Compliance Manager representing the Data Controller, who will arrange the relevant response to that request.

9.3 This Agreement also acts in fulfilment of part of the responsibilities of the Data Controller as required by paragraphs 11 and 12 of Schedule 1, Part II of the Data Protection Act 1998.

Declaration

I agree to abide by the terms and conditions of this agreement. In doing so, I am aware of and understand the relevant provisions of the Data Protection Act 1998, and I agree to abide by these provisions.

Signature of the Data Controller Date

Signature of the Data Processor Date