Data Protection Policy

Document Title: Data Protection Policy			
Version No.	1.1	Policy Owner	LGS
Superseded version		Author Role Title	Deputy Director L&GS
Approval Date	20.01.12 last update 14.03.18	Approved by	EPC
Effective Date	20.01.12	Review Date	14.03.19

Table of Contents

Data Protection Policy

Introduction

In order to carry out its functions, to provide its services and to meet its obligations, the University gathers and processes personal information about its students, staff and other individuals. The University is committed to protecting the privacy of individuals by ensuring the fair, responsible and transparent use of all personal information that it holds, including compliance with the safeguards and requirements of the Data Protection Act 1998. This Policy and its associated Code of Practice and Procedure set out the minimum standards with which all sections of the University must comply in order to satisfy this commitment.

1. Scope

1.1 This Policy applies to all University staff and students, and any other individual authorised to access University information.

1.2 This Policy applies to all recorded information which relates to identified or identifiable individuals, irrespective of the format in which that information is held.

1.3 This Policy does not apply to information processed by the Students' Union, by trade unions, or by any other entities which are located in University premises but are not owned or managed by the University and which have separate legal identities.

2. Objectives

This Policy and its accompanying Procedure and Code of Practice aim to ensure that:

2.1 Personal information gathered and processed by the University is done so fairly, responsibly and transparently, and with full consideration for the confidentiality and privacy of each individual.

2.2 The University complies with all requirements of the Data Protection Act 1998, and all subsidiary or related legislation.

3. Guidance

3.1 This Policy is accompanied by:

3.1.1 a Code of Practice which details the practical implications of the above objectives to University activities including incident management procedures;

3.1.2 A Procedure for Subject Access Requests which outlines the processing of requests for an individual's own personal data.

3.2 Guidance to support the objectives of this Policy is available from Legal & Governance Services) (email: dpa@tees.ac.uk; tel: x.2060) and is also accessible from the Legal & Governance Services intranet available here.

4. Definitions

The following definitions should be applied to the interpretation of this Policy and its accompanying Procedure and Code of Practice:

Personal data, or personal information	Any recorded information relating to an identifiable living individual, including expressions of opinion or intentions.
Sensitive personal data	Any personal data consisting of: racial or ethnic origin, political opinions, religious or other beliefs, membership of a trade union, physical or mental health or condition, sexual life, offences or alleged offences, and proceedings for any offence or alleged offence.
Processing	Any action that can be done with personal data, including but not limited to gathering, using, storing sharing or disposing of personal data.

5. Responsibilities

The University has a corporate responsibility to process personal information with due regard to the rights and freedoms of individuals, and to comply with the requirements of the Data Protection Act 1998. Overall responsibility for this Policy lies with the University Secretary.

Legal & Governance Services has responsibility for providing advice on information compliance issues, for processing and recording requests made under section 7 of the Data Protection Act, for managing relevant complaints, for raising internal and external awareness of the University's obligations, and for maintaining the University's Registration with the Information Commissioner.

Deans and Directors of each School and Department must ensure that the activities and processes within their departments are compliant with this Policy and Code of Practice, and that their staff have a sufficient awareness and knowledge of relevant requirements.

Local Data Protection Coordinators will be assigned within each School and Department by the Dean/Director, with the functions of: providing a local point of contact for DPA issues, and reporting significant changes in the processing of personal data to Legal & Governance Services.

5.1. Responsibilities of Staff

5.1.1. All staff must comply with the requirements of this Policy and Code of Practice.

5.1.2. Staff may only process personal data to the extent to which they have been specifically authorised by the University, or generally authorised as part of their role within the University.

5.1.3. Staff are responsible for ensuring personal data they possess in undertaking their role, is managed securely. Specifically, individual are responsible for ensuring that personal data in their possession is not left unsecure in meeting rooms, public spaces or on desks within open plan environments.

5.1.4. Staff must ensure that existing and new business processes, activities and systems (e.g. IT software) are compliant with the requirements of the Data Protection Act and this Policy and Code of Practice, and that their local Data Protection Coordinator is made aware of any significant changes to the processing of personal data. Specific advice can be provided by Legal & Governance Services as required.

5.1.5. Academic staff are responsible for ensuring that their students are fully informed about their responsibilities under the Act with regard to any specific coursework or research which involves the gathering or processing of personal information. Academic staff authorising the processing of personal information by students for the purpose of coursework or research are responsible for the monitoring of that processing.

5.1.6. Research Ethics Committees will take appropriate measures to ensure that the research activities of students and staff are compliant with Data Protection requirements.

5.1.7. In relation to any processing which is not undertaken in the course of University activities, i.e. where the University is not the Data Controller, individuals are responsible for their own compliance with the Data Protection Act, including Notification with the Information Commissioner if appropriate.

5.1.8. The University's Staff Disciplinary Procedure may be used, if appropriate, should there be a breach of this Policy.

5.2. Responsibilities of Students

5.2.1. In connection with their academic studies/research, all University students have the following responsibilities:

1. to notify an appropriate member of staff, usually their tutor, if they intend to process information about identifiable individuals as part of their academic studies/research;
2. to only process personal information for use in academic studies/research which has been expressly authorised by a member of staff or the appropriate Research Ethics Committee;
3. to comply with any regulations or requirements implemented by the University or by a member of University staff in order to facilitate compliance with the Data Protection Act.

5.2.2. In relation to any activities not specifically authorised by the University, students processing personal data are responsible for their own compliance with the Data Protection Act, including Notification with the Information Commissioner if appropriate.

5.2.3. The University's Student Disciplinary Procedure may be used, if appropriate, should there be a breach of this Policy.

6. Data Protection Principles

6.1. The University will comply with the eight Data Protection Principles as required by the Data Protection Act, which in summary provide that:

1. Personal data must be processed fairly and lawfully, and only when specified conditions are satisfied;
2. Personal data must be processed for specified purposes only;
3. Personal data must be adequate, relevant and not excessive for the purpose;
4. Personal data must be accurate and, where necessary, up-to-date;
5. Personal data must not be kept for longer than necessary;
6. Personal data must be processed in accordance with the rights of individuals;
7. Personal data must be kept appropriately secure;
8. Personal data must not be transferred outside the European Economic Area without adequate protection.

6.2. The accompanying Code of Practice informs the practical application of these Principles to University activities.

7. Rights of Individuals

7.1. The University will comply with the rights given to individuals under the Data Protection Act, which in summary provide that:

1. Individuals have a right of access to their personal data held by the University;
2. Individuals can ask the University to cease processing their personal information for a particular purpose which is likely to cause them substantial and unwarranted damage or distress;
3. Individuals can ask the University to cease processing their personal information for direct marketing purposes;
4. Individuals can object to decisions made solely by automatic means;
5. Individuals can seek compensation if they have suffered damage or distress arising from a breach of the Data Protection Act;
6. Individuals can ask for incorrect or misleading data to be amended.

7.2. Any such enquiries should be referred to Legal & Governance Services, and will be processed in accordance with the relevant statutory requirements.

7.3. The accompanying Procedure outlines the processing of requests for an individuals' own personal data.

8. Registration with the Information Commissioner

8.1. The University, as a Data Controller, maintains a Notification with the Information Commissioner which broadly outlines the data processing activities of the University. This Notification is publicly accessible from the Information Commissioner's website (www.ico.gov.uk); the University's Registration Number is Z5567143. The annual renewal of the Notification is undertaken by Legal & Governance Services.

8.2. All processing of personal information by the University must be covered by this Notification.

9. Relationship with existing Policies, Standards and Legislation

This Policy and its accompanying Code of Practice and Procedure have been formulated with particular reference to the following legislation, guidance and University policies:

- CCTV Policy
- Data Protection Act 1998
- JISC Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998 [Version 3, May 2008]
- Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act [National Archives, 2007]
- British Standard BS10012:2009 – Data protection – Specification for a personal information management system

- Codes of Practice published by the Information Commissioner's Office
- Records Management Policy
- Freedom of Information Policy
- Information Security Policy
- Reference Policy
- Privacy & Monitoring Policy

Data Protection Procedure: Subject Access Requests

Introduction

Individuals ("data subjects") have a general right of access to their personal data which is held by the University. This right is governed principally by the Data Protection Act 1998, which sets out the legal requirements for the processing of such requests (known as "Subject Access Requests").

This Procedure accompanies the University's Data Protection Policy and relates solely to the processing of Subject Access Requests. This Procedure provides a general overview of the processing of such requests. It is important to recognise that there may be specific instances where legislative requirements require the University to deviate from this Procedure in order to comply with those requirements.

Subject Access Requests are coordinated by the Legal & Governance Services; contact details are provided in Section 5 below. Although this Procedure is phrased in terms of a requestor asking for their own personal information, it is recognised that a Subject Access Request may also be submitted by a third party on behalf of an individual.

1. Submitting Subject Access Requests to the University

1.1. Any individual is entitled to ask for copies of information relating to them which are held by the University. Such a request is known as a 'Subject Access Request'.

1.2. The University publishes a template Subject Access Request Form to ease the request process. Requestors are encouraged to use this form to ensure that sufficient information is provided to enable the University to properly and efficiently process such requests. That form is available from www.tees.ac.uk/dpa, or see Section 5 below. The completed form should be submitted to Legal & Governance Services as detailed in Section 5 below.

1.3. If the University's template request form is not used, the request must be made in writing, enclosing evidence of identity and detail of the information requested. The written request should be submitted to Legal & Governance Services as detailed in Section 5 below.

1.4. The University may apply a charge of up to £10 for each request. If no fee is included with the written request, the requestor will be asked to provide it before the request is processed. The University normally charges £2 for accessing all or part of a student/staff file, otherwise the £10 charge will apply. Cheques are payable to "Teesside University"; cash can be

accepted if delivered by hand to Legal & Governance Services (see Section 5 below). Requestors are advised not to send cash through the post.

1.5. The University may request further information in order to be satisfied as to the identity of the requestor or, if different, the consent and identity of the subject of the data. The University may also need to seek clarification as to what information is being sought by the requestor. In such cases the requested information must be supplied before the request can be progressed.

1.6. Once a written request has been received by the University, and any fee or clarification is satisfactorily received, the response must normally be provided within 40 calendar days. This time limit starts when all required information is received by the University.

1.7. In cases where the University has previously complied with a Subject Access Request, it is not obliged to comply with a subsequent identical or similar request unless a reasonable interval has elapsed. Such a decision will consider all the circumstances of the case, particularly the nature of the requested data, the purpose for which it is processed, and how frequently it is changed.

1.8. Legal & Governance Services can provide advice and assistance to requestors in formulating their requests. External advice may be obtainable from the Information Commissioner's Office (www.ico.gov.uk).

2. Internal Processing of a Subject Access Request

2.1. Legal & Governance Services will liaise with relevant Schools/Departments to collate all information relevant to the request. That information will be returned to Legal Services to allow sufficient time for any additional processing that may be necessary. Such processing will include checking for compliance with Data Protection legislation, for example the removal of personal data relating to other individuals as appropriate.

2.2. Where information cannot be provided without disclosing information relating to another identifiable individual, it may be necessary to withhold or anonymise that information in accordance with legislative requirements.

2.3. Members of staff within Schools/Departments who have been asked to supply information to Legal & Governance Services in conjunction with a Subject Access Request should note that:-

a. Any queries or uncertainties as to what information is required should be raised with Legal & Governance Services at the earliest opportunity.

b. If staff are aware of other sources which may hold information relevant to the request, they should make Legal & Governance Services aware.

c. Any withholding or redacting of information which should not be disclosed will be done by Legal & Governance Services prior to disclosure, although staff may wish to identify specific concerns.

d. The identity of a Subject Access Requestor should be considered as confidential information and only disclosed to other individuals where strictly necessary.

3. Responding to a Subject Access Request

3.1. In response to a Subject Access Request, and within the required timeframe (see 1.6 above), requestors will be provided with the following information as appropriate to each request:

a. Confirmation that the University processes the subject's personal data;

b. A general description of: the personal data of which that individual is the data subject, the purposes for which that data is processed, any information available as to the source of that data, and the classes of recipient to whom that data may be disclosed;

c. Copies of information constituting personal data of which that individual is the data subject (see 3.4 below).

3.2. Where appropriate to the information provided, an explanation of any codified or other unintelligible information will be included.

3.3. Where applicable to the request, the requestor will also be provided with information about the logic involved in any data processing which evaluates matters relating to the data subject, where such processing is automated and constitutes the sole basis for any decision which significantly affects the data subject.

3.4. The disclosure of personal data in response to a Subject Access Request will normally be made in permanent form, either paper or electronic. However in cases where it is not possible to provide copies in permanent form, or where such provision would involve disproportionate effort, or where the data subject agrees accordingly, access to such data may be arranged through another format, for example viewing the information in person.

4. Complaints relating to Subject Access Requests

Any individual who is dissatisfied with the way in which the University has handled a Subject Access Request should put their concerns in writing to the Assistant Director (Legal Services), using the contact details below.

5. Contact Details

For queries or advice in relation to Subject Access Requests, or other matters relating to Data Protection at the University, please contact Legal & Governance Services as below.

By post: Legal & Governance Services
Information Compliance Team
Teesside University
Middlesbrough
TS1 3BA

By phone: 01642 342060

By email: dpa@tees.ac.uk

In person: Second floor of the Student Centre building. Please phone in advance to ensure that someone will be available to meet with you.

Data Protection Code of Practice

Contents

Introduction

This Code of Practice accompanies the University's Data Protection Policy and puts into practical terms the requirements that must be followed in order to fulfil the objectives of that Policy and to adhere to legislative requirements.

1. Data Processing Statements

1.1. The University publishes Data Processing Statements which provide broad information about how the University processes the personal information of its students and staff. The staff statement is published on the intranet and distributed to new staff at induction; the student statement is published on the internet and in the University Student Handbook. Both Statements are available from the Legal Services intranet or by contacting Legal Services.

2. General requirements when processing personal information

2.1. This section applies to any processing of personal information, including gathering, using and disclosing it.

2.2. Personal information must be processed fairly at all times. This requirement includes:

- being open and transparent about how personal information is used (see section 4 below);
- handling personal information only in ways would be reasonably expected by the individuals concerned;
- not processing personal information in ways which would have unjustified adverse effects on the individuals concerned;
- only processing personal information where it is necessary for legitimate purposes;
- not doing anything unlawful with personal information.

2.3. Personal information may only be processed when one of the criteria specified in Schedule 2 of the Data Protection Act can be satisfied. Summaries of the most relevant criteria are that:

- the individual has given their consent (nb consent may not be inferred from a lack of objection);
- the processing is necessary for the fulfilment of a contract to which the individual is a party;
- the processing is necessary for compliance with a legal obligation;
- the processing is necessary for the purposes of legitimate interests pursued by the University, and does not prejudice the rights or interests of the individual.

2.4. Personal information which has been obtained for a specific purpose may not be further processed for any incompatible purpose.

2.5. Personal information processed for any purpose must be adequate, relevant and not excessive for that purpose.

2.6. Reasonable measures should be taken to ensure that personal information is accurate and, where necessary, up-to-date.

2.7. Personal information must be kept appropriately secure at all times, with precautions appropriate to its confidentiality and sensitivity. Particular care must be taken when processing personal information at home or at another off-site location, as such processing presents an increased risk of loss, theft or damage to that information.

2.8. When processing information about identifiable individuals, it may be appropriate to consider the distinction between ‘professional’ and ‘private’ information. For practical purposes, information relating to an individual’s professional capacity, e.g. University contact details or job title, will be subject to less stringent privacy considerations than information of a more private nature, e.g. home contact details.

2.9. In cases where personal information is processed by another organisation on behalf of the University, Legal Services must be consulted to ensure legislative compliance.

3. General requirements when processing sensitive personal information

3.1. "Sensitive personal data" is defined by section 4 2 of the Data Protection Policy as encompassing any personal data consisting of: racial or ethnic origin, political opinions, religious or other beliefs, membership of a trade union, physical or mental health or condition, sexual life, offences or alleged offences, and proceedings for any offence or alleged offence.

3.2. Particular care must be taken with the gathering, use, storage, disclosure and destruction of this category of information.

3.3. In addition to each of the requirements in section 2 above, sensitive personal data may only be processed when one of the criteria specified in Schedule 3 of the Data Protection Act can also be satisfied. Summaries of the most relevant criteria are that:

- the individual has given their explicit consent;
- the processing is necessary for a legal obligation in connection with employment;
- the processing relates to racial or ethnic origin, it is necessary for monitoring equal opportunities, and is carried out with appropriate safeguards for the rights of the individuals.

4. Gathering Personal Information

4.1. Personal information must be adequate and relevant for the specific purpose for which it is gathered. Only the minimum necessary information should be gathered to satisfy that specific purpose.

4.2. When data is gathered from individuals the information below must be made clear to them:

- The identity of the Data Controller (i.e. the University, not individual departments);
- the purpose for which the data will be processed;
- any other information that may be relevant to support "fair" processing, e.g. foreseeable external disclosures.

4.3. This will normally be achieved in the form of a Privacy Notice (also known as a Fair Processing Notice). This applies however personal information is gathered from individuals, whether via paper forms, online forms, information provided verbally, or other means, and seeks to ensure that any subsequent processing can be "reasonably expected" by the individual. Further guidance and advice on Privacy Notices is available from Legal Services.

4.4. Where a Privacy Notice is supplied to an individual, a record of that Notice should be kept for as long as the personal information is retained.

4.5. Where practicable, a record should be kept of the circumstances in which the personal information was obtained (e.g. when and how).

5. Storing and Disposing of Personal Information

5.1. Personal information must always be kept appropriately secure against damage or unauthorised access, amendment or deletion, with precautions appropriate to its confidentiality and sensitivity.

5.2. Electronic and physical files should have appropriate access restrictions in place so that only authorised individuals can gain access to them.

5.3. Personal information must not be stored on portable media devices (e.g. memory sticks, DVDs) unless this is essential to serve a particular legitimate short-term purpose. Such devices are particularly susceptible to damage, loss or theft.

5.4. Where personal information needs to be stored on a portable media device, and is either "sensitive personal data" as defined in the Data Protection Policy, or the loss of that information would otherwise cause damage or distress to an individual, that information should be encrypted using facilities provided by the University.

5.5. Personal information must not be kept for longer than is necessary. Be particularly aware of electronic databases building up indefinitely. The University's Record Retention Schedule guides the retention requirements for records relating to various activities.

5.6. Personal information must be disposed of in a manner appropriate to its sensitivity. Records awaiting destruction must continue to be stored securely.

5.7. All staff are required to follow the Confidential Waste Disposal Procedure set out in Appendix 3.

6. Disclosing and Sharing Personal Information

6.1. As a general rule, personal information may not be disclosed to any third parties without the consent of the individual concerned, or authorisation from either Legal & Governance Services or Human Resources as appropriate. In this context "third parties" includes, but is not limited to, family members, friends, local authorities, government bodies and the police.

6.2. Requests for the disclosure of personal data about staff or students, from the police, the Student Loans Company, or from other official bodies and agencies must be referred to the Legal & Governance Services so that a lawful basis for sharing the information can be demonstrated. The exception to this is in cases where the immediate disclosure of personal data is required by law enforcement agencies or health care agencies for the imminent prevention of crime or prevention of harm to an individual and

Legal & Governance Services are unavailable or cannot be contacted (e.g. outside of standard working hours). In cases where a disclosure is made, staff should ensure that Legal & Governance Services are contacted at the next available opportunity with details of the disclosure.

6.3. The provision of references is the subject of a separate University policy.

6.4. Personal information can be shared within the University provided that such sharing is reasonable, necessary, not excessive, and is not incompatible with the original purpose for gathering the data.

6.5. When disclosing or discussing information about individuals, reasonable steps should be taken to verify the identity of the recipient, especially in telephone conversations or email correspondence. Be aware of the risk of individuals posing as apparently legitimate recipients in order to acquire information from the University.

6.6. When disclosing or sharing personal information, particular care must be given to the risks of correspondence being intercepted or errors in transmission. Only the minimum necessary information should be included and particular care must be taken when entering the recipient's details. If appropriate to the sensitivity of the information, email attachments can be password protected and/or encrypted.

7. Personal Data Breach

7.1. A personal data breach is considered to be any loss, damage or destruction to personal data or the unauthorised access, disclosure and/or processing of personal data.

7.2. Such incidents may constitute a breach of the Data Protection Act 1998 for which the University can be subject to financial penalties of up to £500,000 and which can result in damage or distress being caused to our customers. It is therefore vital that such incidents are reported and investigated in a timely fashion.

7.3. To ensure that breaches can be investigated and managed they must be reported to the Information Compliance Team in Legal & Governance Services without delay using the Personal Data Incident Form available here https://itservicedesk.tees.ac.uk or by calling ext. 2563.

7.4. For the purpose of this policy, reporting requirements cover actual and suspected breaches.

7.5. Examples of personal data breaches include:

7.5.1. Loss or theft of devices or equipment on which personal data is stored e.g. a memory stick;
7.5.2. An email containing personal data sent to the wrong person;
7.5.3. Disclosure of personal data, via any method, to a third party such as a family member without consent or another legal power or obligation to do so.

7.5.4. A member of staff who has accessed the personal records of family or friends without their consent.

7.6 If you are unsure whether an incident constitutes a breach, please contact the Information Compliance team for advice.

7.7 The Information Compliance Team will determine how the breach should be investigated and managed, in line with the following principles:

7.7.1 Containment and recovery: decide who will investigate and ensure that any immediate actions are undertaken to limit potential damage.
7.7.2 Risk assessment: understand the potential impact of the breach, both to the individuals concerned and to the University.
7.7.3 Notification: consider whether any individuals or organisations should be notified that a breach has occurred.
7.7.4 Evaluation and response: finalise the investigation, understanding the cause of the breach and considering further actions that might be required to prevent future recurrence.

7.8 The reporting Manager will be required to support actions to manage a breach. This may include, amongst other actions, recovery of lost personal data or devices, analysis of root causes and changes to procedure to prevent recurrence.

8. Complaints

8.1. Any complaints, concerns or dissatisfaction regarding the University's processing of personal information must immediately be brought to the attention of the Executive Director (Legal & Governance Services).

9. Contacts and Further Information

9.1. Queries relating to the processing of personal information or the Data Protection Act should be referred either to Legal & Governance Services or Human Resources as appropriate.

9.2. Further guidance on relevant issues is available from Legal & Governance Services (email: dpa@tees.ac.uk; tel: x.2060) and is also accessible from the Legal & Governance Services intranet available here InformationCompliance/DataProtection.

Confidential Waste Disposal Procedure

1. Introduction

The objective of this procedure is to prevent loss, theft or compromise of confidential paper waste.

2. Scope

2.1. The University requires that all confidential waste is disposed of securely and appropriately in accordance with current legislation.

2.2. The University requires that records should be kept only as long as they are required for corporate business or legal reasons. At the end of this period records should be disposed of.

2.3. The appropriate time for keeping most records can be found in the University Retention Schedule. The Retention period applies equally to all media, including electronic. A record should be kept of all University records which you destroy. Note it may be a criminal offence to destroy records inappropriately.

2.4. Not all information is a record but may still require secure disposal. Examples of records or information that should be confidentially disposed of include but not limited to:

2.4.1. Personal data – names, addresses, date of birth, etc.
2.4.2. Bank details sometimes these may not be personal data but should always be treated as such
2.4.3. Copy documents – containing personal or confidential data
2.4.4. Working papers – containing personal or confidential data
2.4.5. Draft documents – containing personal or confidential data

2.5. Secure destruction is an expensive procedure and therefore non-confidential paper waste should be disposed of in the paper recycling bins.

3. **Responsibilities**

3.1. Heads of Service, Deans/Directors

3.1.1. ensuring that confidential paper waste is disposed of in line with this procedure;
3.1.2. ensuring that the destruction of the corporate records has appropriate authority and maintaining an appropriate record of the authority and what has been destroyed has been kept;
3.1.3. that records are destroyed in accordance with the Retention Schedule – unless they are duplicates and not required;
3.1.4. Notifying Campus Services if any Confidential Waste Unit (CWU) is full.

3.2. All Staff

3.2.1. Disposing of confidential waste appropriately;
3.2.2. Notifying Campus Services if any CWU is full.

3.3. Procedure

3.3.1. CWU units have been placed around site. All units are completely emptied on a regular and auditable schedule within recommended confidential waste industry timescales. This ensures that confidential waste is not stored for any longer than necessary.
3.3.2. Units are emptied by Contractor staff on a scheduled basis. Extra bags and boxes should be removed at the same time.
3.3.3. Units, bags etc. are removed from University sites in a secure tracked vehicle.
3.3.4. Material is subjected to an offsite secure destruction process to confidential waste industry specification and monitored by CCTV.
3.3.5. After destruction, the waste is recycled and destruction and environment certificates are issued to the University.
3.3.6. In exceptional circumstances a CWU may be opened. Should there be a requirement to open a CWU other than during the scheduled collection a written request should be sent by the relevant Head of Service to the Information Compliance Team dpa@tees.ac.uk.