UNIVERSITY COLLEGE
OF ESTATE MANAGEMENT

UCEM Data Protection Policy

This policy should be read in conjunction with the Remote Working Policy and Information Security Policy

Reference:	
Version:	6.00
Status:	Final
Author:	Liz Howlett
Date:	06/12/2017

Approval History

Version	Date	Name
3	12/09/2017	Senior Leadership Team
4	18/10/2017	GDPR Working Group
5	09/11/2017	GDPR Working Group
6	06/12/2017	Board of Trustees

Document History

Version	Date	Reason	Person
00.01	31/07/2017		
00.02	04/08/2017	Guidance moved to appendices	Liz Howlett
00.03	12/09/2017	Highlighting questions and updating	Liz Howlett
00.04	10/10/2017	Incorporating comments from consultation with GDPR Working Group	Liz Howlett
00.05	09/11/2017	Comments from GDPR Working Group meeting	Liz Howlett
00.06	06/12/2017	Board of Trustees	Liz Howlett

UCEM Policy

Data Protection Policy

Table of Contents

1. Introduction

The Data Protection Act 1998 ('DPA 1998') protects the rights of individuals to have their personal data collected and stored securely and used only for legitimate and lawful purposes for which their consent has been sought. The General Data Protection Regulation 2016 ('GDPR') will become part of UK law from 25th May 2018. The Data Protection Act 2018 ('DPA 2018') will replace the DPA1998. The GDPR updates the law taking into account technological changes. It improves the rights of individuals and increases the accountability of organisations.

This policy sets out how the University College of Estate Management ('UCEM') complies with the Data Protection Act 1998 and how it will comply with the GDPR and the DPA 2018. The policy will be reviewed and updated at least annually. This policy applies across all territories and jurisdictions in which UCEM operates.

UCEM collects personal data for many reasons. We must process data to run our business and to provide the best possible service to our students.

The kind of records that we keep of our students, staff (includes employees and temporary workers), contractors and Board members are listed below (this is not an exhaustive list). We collect this data to allow us to meet statutory, regulatory and audit requirements, and to run our business effectively.

Students (including alumni)	**Staff/ Board members (including former staff)**
Contact details	Job application documents and forms
Application forms	References received and given
Apprenticeship Application forms	Next of kin details for emergency contact
Apprenticeship Commitment Statement	Payroll and tax information
Apprenticeship Delivery Agreement	Planned and unplanned absence records including sickness records
Individualised learner record return	Medical and health information
Risk assessments	Job performance and probation records
Definitive Award information	Records relating to promotion or transfer
Complaints data	Training and development records
Equality and diversity information	Disciplinary records
Information provided by third parties	Record of service
Survey results (e.g. DLHE)	Health and safety information
Mentormatchme	Records relating to accident or injury at work
Mitigating circumstances documents	Contact details and payment details
Academic misconduct information	
Passport and financial details	
Additional Support Agreements	

UCEM holds, and processes, personal information and therefore registers with ("notifies") the Information Commissioner as a "data controller". The Information Commissioner is responsible for overseeing information legislation and will be the relevant supervisory authority under the DPA 2018.

2. Monitoring and Review

This policy has been approved by the Senior Leadership Team and the Board of Trustees.

It will be reviewed with other information compliance policies and guidelines annually and the responsibility for review will rest with the Senior Leadership Team followed by approval by the Board of Trustees.

The Board delegates authority to the GDPR Working Group to update the policy, if required, to reflect the guidance from the ICO on GDPR compliance which is not yet available, and the provisions of the Data Protection Bill which is still being debated. Any policy decisions as a result of the updated guidance from the ICO must be referred to the Senior Leadership Team for a final decision.

Vice-Principals and Deans are responsible for ensuring this policy is observed within their departments. Local support is provided by the Information Champions (see 4.4).

If anyone considers the policy is not being followed they should raise this with the Data Protection Officer (see 4.3).

3. Your Rights

You have the right: to ask UCEM for a copy of your personal data (a data subject access request) as detailed in Appendix One.

You also have the right to object to processing that is causing you, or is likely to cause you, damage or distress; to object to communications or direct marketing; in certain circumstances to require us to correct or erase your personal data (this right is subject to the application of a public interest test); and a right to compensation for damages caused by a breach of the DPA 1998.

UCEM will retain student data indefinitely or until a student requests us to do otherwise. We will publish on our website any changes we make to this data protection policy and notify you by other communication channels where appropriate. You have the right to lodge a complaint with the Information Commissioner's Office at https://ico.org.uk/concerns/

Where you exercise your right to erasure, we will continue to maintain in respect of past students a core set of personal data (name, subject(s), record of learning and achievement and award details, unique UCEM identification number and date of birth) to ensure we do not contact you inadvertently in future, while still maintaining our record of your academic achievements. We may also need to retain some financial records about you for statutory purposes (e.g. Gift Aid, anti-fraud and accounting matters). We will apply the public interest test when considering any request to delete personal data.

4. Definitions

4.1 Personal Data

Personal data means data which relates to a living individual who can be identified –

(a) from that data, or

(b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data". It also includes opinions about the individual.

The more expansive definition in the DPA 2018 includes online identifiers and provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

4.2 Sensitive personal data

Sensitive personal data (or 'special categories of personal data' under the GDPR) relates to:

(a) the racial or ethnic origin of the data subject,

(b) their political opinions,

(c) their religious beliefs or other beliefs of a similar nature,

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) their physical or mental health or condition,

(f) their sexual life,

(g) the commission, or alleged commission, by them of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the DPA 2018 depending on how difficult it is to attribute the pseudonym to a particular individual. This is relevant for UCEM where we use UCAS generic codes to record medical conditions.

The categories of data are broadly drawn so that, for example, information that someone has a broken leg is classed as sensitive personal data, even though such information is relatively matter of fact and obvious to anyone seeing the individual concerned. Clearly, details about

an individual's mental health, for example, are generally more 'sensitive' than whether they have a broken leg. We will record any agreement to include sensitive data in records of conversations with students.

4.3 Data Protection Officer

The responsibility of the Data Protection Officer ('DPO') is as follows:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and DPA 2018 and other relevant laws.
- To monitor compliance with the DPA 2018 and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, students etc)

UCEM ensures that the DPO:

- Reports to the highest management level – i.e. Board level.
- Operates independently and cannot be dismissed, or penalised, for performing their task.
- Has adequate resources to enable them to meet the obligations under the DPA 2018

4.4 Information Champions

To support the DPO there are Information Champions in each area. The Information Champion will represent their area on UCEM's GDPR Working Group and will provide support and assistance to the DPO.

The role involves:

- Being the key contact in their area for data protection queries and signposting colleagues to further detailed advice and support
- Promoting best practice including new guidelines and ways of working. This includes ensuring that the changes under the GDPR and the Data Protection Act 2018 are understood and implemented in their area.
- Knowing about the information that is held in their area, why it is held and who should (and should not) have access to it.
- Guiding and supporting staff in their area in managing information risk.
- Being part of an active network across UCEM learning and supporting each other and providing support to the DPO.

4.5 Consent

Consent under the DPA 2018 must be freely given, specific, informed and an unambiguous indication of an individual's wishes. There must be some form of clear affirmative action – a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there must be a simple way for people to withdraw consent.

5. Data Protection Principles

The data controller (UCEM) shall be responsible for, and able to demonstrate compliance with, the following principles:

5.1 Processed lawfully, fairly and in a transparent manner

This means that we must:

- have legitimate grounds for collecting and using your personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle the personal data of both students, employees and contractors only in ways they would reasonably expect; and
- make sure we do not do anything unlawful with the data.

The lawful basis for the processing of data by UCEM is that processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract and/or has been carried out with the consent of the data subject.

There are two specific areas where UCEM will process special categories of personal data. These are where:

- processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of an employee or student, medical diagnosis, the provision of health or social care or a contract with a health professional or a non-medical help supplier
- processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

5.2 Collected for specific, explicit, legitimate purposes

It shall not be further processed in a manner that is incompatible with those purposes but further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. UCEM supplies statistical data to the Higher Education Statistics Authority (‘HESA’) and to other statutory bodies for the purposes of monitoring outcomes. We will tell individuals when this will be done and why.

Please see Appendix Six for the HESA Student Collection Notice.

5.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

This means we must ensure that the personal data held is sufficient but that no more is held than we need. We will not hold information that we will never need but we may hold information for a foreseeable event that never occurs.

We will identify the minimum amount of personal data we need to properly fulfil our purpose. We will hold that much information, but no more.

5.4 Accurate and, where necessary, kept up to date.

Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay

5.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the DPA 2018 in order to safeguard the rights and freedoms of individuals

5.6 Processed in a manner that ensures appropriate security of personal data.

This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

6. Information security

Security is a critical part of keeping information confidential. UCEM take steps to ensure that all information is held securely both physically and electronically. Appendix Four details our security procedures and Appendix Five details the procedure for dealing with any breaches of information security.

Please see the UCEM policies on Remote Working and on Information Security

7. Data Sharing

There are two types of data sharing: systematic and exceptional

'Systematic' means a routine sharing of data or pooling of data.

'Exceptional' is one-off sharing (which might have to happen in an emergency)

When deciding whether to share data UCEM will consider the following:

• **What is the sharing meant to achieve**? We will have a clear objective, or set of objectives. Being clear about this allows us to work out what data we need to share and who with. We will document this.

• **What information needs to be shared**? We won't share all the personal data we hold about someone if only certain data items are needed to achieve our objectives.

• **Who requires access to the shared personal data**? We employ 'need to know' principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This will also address any necessary restrictions on onward sharing of data with third parties.

• **When should it be shared**? Is this an on-going, routine process or should it only take place in response to particular events?

• **How should it be shared**? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

• **How can we check the sharing is achieving its objectives**? We will judge whether it is still appropriate and confirm that the safeguards still match the risks.

• **What risk does the data sharing pose**? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in us?

• **Could the objective be achieved without sharing the data or by anonymising it**?

• **Do we need to update our notification**?

• **Will any of the data be transferred outside of the European Economic Area (EEA)**?

7.1 Routine data sharing

Data will be shared routinely with government departments, specifically the Education and Skills Funding Agency ('ESFA') (apprentices only) and the Higher Education Statistics Authority ('HESA'). When students register with us they consent to this sharing of data.

Where data is shared routinely with other organisations a data sharing agreement will be in place.

7.1.1 Data sharing agreements

These will, at least, document the following issues:

• the purpose, or purposes, of the sharing;

• the potential recipients or types of recipient and the circumstances in which they will have access;

• the data to be shared;

- data quality – accuracy, relevance, usability etc;
- data security;
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by individual staff.

7.1.2 Points we will consider before sharing:

Is the format of the data being shared compatible?

The IT team is consulted about the secure transfer of data and, if a data sharing agreement is required, the IT team are also consulted to ensure all IT requirements are acceptable, and can be delivered. The format of the data being shared must be compatible with the systems used by all those sharing. We will check that information is held in the same way and that it is accurate. If we need to share data urgently, we will test how well the systems used for sharing the data work when it is not urgent.

Is the information we are sharing accurate?

We will agree how any incorrect data will be corrected by all parties

Agree common retention and destruction arrangements for the data sent and received

Staff in the area affected will be sufficiently trained to know when to share data and in what circumstances

7.2 Exceptional data sharing

UCEM complies with the Social Care Institute for Excellence guidelines on sharing information including compliance with the Prevent duty under the Counter-terrorism and Security Act 2015. Information will be shared with the right people at the right time to:

- Prevent death or serious harm
- Coordinate effective and efficient responses
- Enable early interventions to prevent the escalation of risk
- Prevent abuse and harm that may increase the need for care and support
- Maintain and improve good practice in safeguarding students
- Reveal patterns of abuse that were previously undetected and that could identify others at risk of abuse
- Identify low-level concerns that may reveal people at risk of abuse
- Help people to access the right kind of support to reduce risk and promote wellbeing
- Help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- Reduce organisational risk and protect reputation

8. CCTV

CCTV is closed circuit television. This is a private television system involving one, or more, cameras connected to one, or more, monitors for security, surveillance, law enforcement and

general-purpose monitoring applications. Unlike public broadcast TV, it is a closed system intended for private use.

The personal information we collect includes CCTV images. This is to provide a safe and secure environment for all staff and visitors at Horizons. We aim to deter and prevent crime. We aim to identify, apprehend and prosecute offenders and identify actions where disciplinary action might be needed. CCTV protects our buildings and staff.

Recorded material is stored in a way that maintains the integrity of the information.

It is kept securely and access is restricted.

Recorded images will be viewed in a restricted area.

The retention period is informed by the purpose for which the information is collected.

It is not kept for longer than is necessary.

9. Cookies

If you use the internet to carry out certain transactions with UCEM, your computer will store small pieces of information, known as 'cookies', in its memory. Cookies cannot read your computer's hard disk or make any information available to third parties. They are used so that we can easily recognise you when you return to our websites and, as a result, will enable us to provide you with a better service. We also track user traffic patterns in order to determine the effectiveness of our website. We do not release this information to third parties. If you prefer not to receive cookies while browsing our website, you can set your browser to refuse them. However, if you are a registered student with UCEM you will need to allow "per-session" cookies in order to access password-protected sites.

10. Contact details

If you have any queries or concerns about the handling of your personal data please contact the Data Protection Officer at:

dataprotection@ucem.ac.uk

If you remain dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner. There is no charge for making an appeal. Contact details are:

The Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 01625 545745 or 0303 123 1113 (local rate) or email: casework@ico.gov.uk

Appendix One

‘Subject Access Requests’

Who can access information?

UCEM will make sure that only people that need personal information can have access to it. An individual can make a “subject access request” about themselves. If a third-party requests information about an individual, the individual must give informed consent to the third party seeking that information. Sponsoring employers will have explicit consent to see the name, date of birth, unique UCEM reference number, programme of study, progress and results of sponsored employees.

Personal information held on employees will only be disclosed to members of the HR department, their own line manager, or a senior manager where specific action is required. If an employee accesses another employee’s records without authority, this is deemed an act of gross misconduct under our disciplinary policy and is a criminal offence under section 55 of the DPA 1998.

Personal information held on Board members will only be disclosed to the HR department, members of the Executive Support team who deal with board administration, or Deans or Vice-Principals, should any action need to be taken in relation to conduct.

Identity Validation

To ensure that information is only disclosed to people who are entitled to see it the identity of the person requesting the information will be validated before disclosure.

Prospective Student

When receiving a request for information by any means information will only be disclosed if the following checks are passed:
Either

- a valid application number has been supplied.
- the name supplied matches the name held against the application.
- If an email address is supplied it must match to an email held against the application

Or

- the following information is supplied and matches to an application: name, date of birth, programme applied for, approximate date of application (+/- 2 years).

Current Student

When receiving a request for information by post or email information will only be disclosed if the following checks are passed:

- A valid student number has been supplied.

- The name supplied matches the name held against the student number.
- If an email address is supplied it must match to an email held against the student.

When a request for information is made over the phone the identity of the caller will be verified by:

- Obtaining a valid student number.
- Obtaining a name that matches to the student number.
- Obtaining the name of the programme they are studying.
- If there is any doubt the date of birth should also be checked to confirm identity.

If a student is unable to supply their student number then the following information should be supplied and should match to the record on SITS before disclosing the student number:

- Full name.
- Email address.
- Data of birth.
- Programme being studied

Past student

When receiving a request for information by any means information will only be disclosed if the following checks are passed:

Either

- a valid student number has been supplied.
- the name supplied matches the name held against the student number.
- If an email address is supplied it must match to an email held against the student.

Or

The following information is supplied and matches to a record on SITS:

- name when studied at UCEM,
- date of birth,
- programme studied,
- approximate date of graduation (+/- 2 years).

Approved Third Party

This is when a student has given permission for a third party to access their information in writing and the approval has been verified as coming from the student.
The third party must provide the following information in all communication and this must match to the information held against the student:

- Student number and/or date of birth
- Student name whilst registered as a student
- Third party name.
- Third party relationship with student.
- Signed/dated authorisation

Current Member of Staff

When receiving a request for information from a current member of staff the request must either come from the staff member's email address or be made in a 1-1 meeting with the staff member, either verbally or by the handing over of a written request.

Past Member of Staff

When receiving a request for information from a past member of staff the person should be requested to supply a full name

Other Contact on Database

UCEM holds information on suppliers, course delegates and other people who have worked with UCEM or who are marketed to by UCEM. If a request is received from one of these individuals for information by default provision of a name and address or name and email address that matches our records is viewed as sufficient information to identify them.

Making a subject access request

All staff members are trained in data protection as part of their induction and on an ongoing basis so will be able to recognise a request for personal data and will pass it immediately to the DPO.

Appendix Two contains a flowchart for the process of dealing with a subject access request.

How to make the request

The request should be in writing and should be made by the individual (the data subject) unless they have authorised a third party to make the request. The identity validation process set out above will ensure that personal information is only disclosed to someone who has the right to see it.

What you are entitled to

Subject access entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- told whether any personal data is being processed – so, if we hold no personal data about the requester, we must still respond to you to let you know this;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- given details of the source of the data (if known).

What we will do

The request will be logged in the Subject Access Request log on the SharePoint system. The log will record the date and time the request was received, who it was received from, the staff member who received the request and a reference number for the request will be allocated.

Frequent requests

The DPA 1998 allows some discretion when dealing with requests that are made at unreasonable intervals. It says we are not obliged to comply with an identical or similar request to one we have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones. Although there is no statutory definition of a reasonable interval as it depends on factors such as how often the data is updated we will generally consider a reasonable interval to be within the last three months. A search of previous requests will be made to ensure that this is not a similar request to one made previously. Legal advice will always be sought if a request is to be refused. The DPA 2018 will have grounds for refusing on the basis of 'manifestly unfounded or excessive' requests.

'Disproportionate effort'

The 'disproportionate effort' exception is in section 8(2) of the DPA 1998. The Court of Appeal has provided clarification as to its application in its 2017 judgments in the cases of Dawson-Damer & Ors v Taylor Wessing LLP [2017] EWCA Civ 74 2 and Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd & Ors; Deer v University of Oxford and University of Oxford v Deer.

The DPA 1998 does not define 'disproportionate effort', but the court has determined that there is scope for assessing whether, in the circumstances of a particular case, complying with a request by supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's right of access to their personal data.

The courts have also made it clear that in assessing whether complying with a Subject Access Request would involve disproportionate effort under section 8(2)(a) we may take into account difficulties which occur throughout the process of complying with the request, including any difficulties we encounter in finding the requested information.

If the request for information is very vague clarification can be sought as to what is being requested. If such clarification is sought this should be noted in the Subject Access log on SharePoint.

Finding the information

The DPO will coordinate the response but may need to contact the Information Champions in each area who will be responsible for searching the records in their area and providing the information to the DPO.

Timescales

The time period for dealing with a SAR is 40 calendar days but this will be one month under the DPA 2018. UCEM will endeavour to respond as soon as possible.

Format and exemptions

The DPO is responsible for deciding what information should be disclosed, what exemptions should be applied (see below) and what format the response should be sent in. UCEM will try to provide information in the format which has been requested but cannot guarantee that this will always be possible or practical.

Where exemptions are applied legal advice will be sought. Possible exemptions include (this list is not exhaustive and is subject to changes which will be made under the DPA 2018):

- References given (not received)
- Publicly available information
- Management information (such as restructuring or possible redundancies)
- Negotiations with the requestor
- Legal advice and proceedings
- Third party data (see Appendix Three for details)

Exemption for requests for information about the outcome of academic, professional or other examinations

These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results. Information comprising the answers given by a candidate during an examination is exempt from the right of subject access. A Subject Access Request ('SAR') cannot be used to obtain a copy of an individual's examination script. Although this exemption does not extend to an examiner's comments on a candidate's performance in an examination (whether those comments are marked on the examination script or recorded on a separate marking sheet), or to details of the marks awarded, there is a special rule governing the time limit for responding to a Subject Access Request for such information in cases where the Subject Access Request is made before the results are announced. In such cases, a response must be provided within the earlier of:

- five months of the date of the request; and
- 40 days of the date on which the results are announced.

Where a request is made for an individual's examination marks, a response may only be refused (or delayed) for reasons permitted by the legislation. We would not refuse to provide details of examination marks in response to a Subject Access Request because the requester had failed to pay their tuition fees. Clearly, though, providing information about examination results is not the same as conferring a qualification.

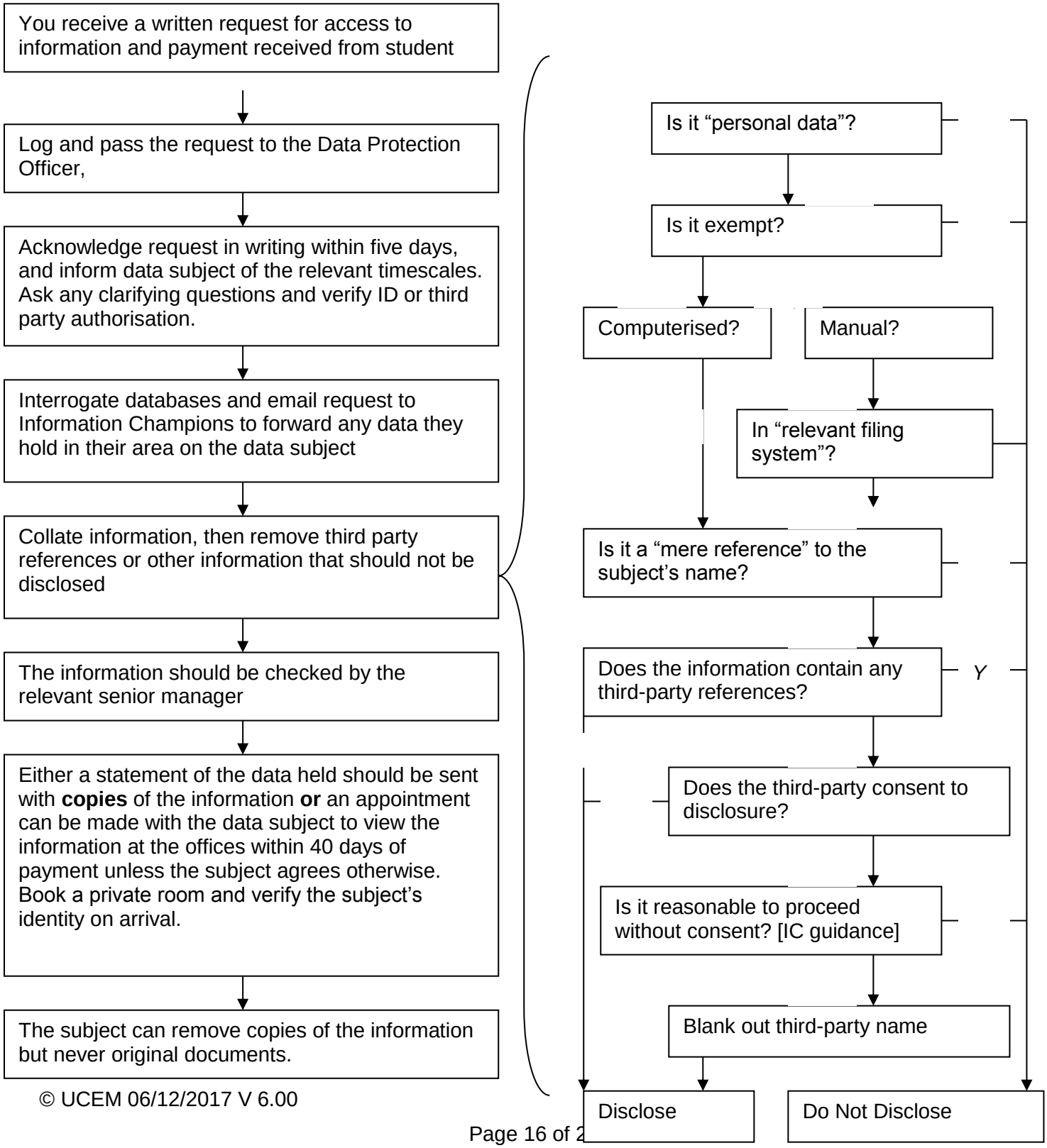
Sending the information

A full audit trail will be maintained by the DPO of exemptions applied and how decisions about what should be disclosed have been taken.

When the information is sent the SAR log on SharePoint will be updated confirming date and time the information was sent. A copy of the information supplied will be retained by the DPO.

Appendix Two

Request for personal information flowchart



Appendix Three

Third Party Data

The Data Protection Act 1998/2018 says we do not have to comply with a Subject Access Request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or

- it is reasonable in all the circumstances to comply with the request without that individual's consent.

This will remain the case under the GDPR. Although we may sometimes be able to disclose information relating to a third party, we need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to us disclosing the information about them, it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway.

Step 1 – **Does the request require the disclosure of information that identifies a third party?**

Is it possible to comply with the request without revealing information that relates to and identifies a third-party individual? We must take into account the information we are disclosing and any information we reasonably believe the person making the request may have, or may get hold of, that would identify the third-party individual.

The obligation is to provide information rather than documents, so we may delete names or edit documents if the third-party information does not form part of the requested information. However, if it is impossible to separate the third-party information from that requested and still comply with the request, we will take account of the following considerations.

Step 2 – Has the third-party individual consented?

In practice, the clearest basis for justifying the disclosure of third party information in response to a Subject Access Request is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a Subject Access Request. However, we are not obliged to try to get consent and in some circumstances, it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. It may not always be appropriate to try to get consent, for instance if to do so would inevitably involve a disclosure of personal data about the requester to the third party.

Step 3 – Would it be reasonable in all the circumstances to disclose without consent?

In practice, it may sometimes be difficult to get third-party consent, e.g. the third party might refuse consent or might be difficult to find. If so, we

must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway.

The Data Protection Act 1998 provides a non-exhaustive list of factors to be taken into account when making this decision. These include:

- any duty of confidentiality owed to the third-party individual;
- any steps you have taken to try to get the third-party individual's consent;
- whether the third-party individual is capable of giving consent; and
- any stated refusal of consent by the third-party individual.

Confidentiality is one of the factors you must take into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where information that is not generally available to the public has been disclosed to you in the expectation that it will remain confidential.

The following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and patient)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

There will be new guidance from the ICO on Subject Access Requests at the end of 2017/beginning of 2018 and this policy will be amended to reflect this

Appendix Four

Information Security

Buildings

We take the following measures to make sure the information we keep is secure within our buildings, and that unauthorised people cannot access it:

- Controlled access to buildings
- ID cards for staff
- Intruder alarms
- CCTV
- Out of hours access policy
- Visitors registered and escorted whilst in the building

Documents

The following guidance helps to keep documents secure:

- Paper file covers are marked with “Confidential” plus “Human Resources”, “Financial”, “Legal” or “Administrative” to classify the contents and retention instructions
- Strong passwords are used, at least seven characters, upper and lower case, using numbers and special keyboard characters (such as currency symbols)
- Passwords are not shared
- You should only be able to access the information you need to do your job. Please contact your manager if you come across personal data that is not secure.
- If you hold confidential files keep them in a locked cabinet and never leave them in open trays or on desktops at the end of the day, or while you are away from your desk.
- If you are away from your desk you should “lock” your computer. You can do this by pressing “ctrl + alt + delete” and then choosing “lock” (or start symbol and L). Staff are accountable for all computer activity and transactions made under their user ID, whether they are present or not.
- Before a file is archived make a note of the date for destruction (or review) on the paper, or electronic, file. This should be x years from the date of closure of the file.
- Files should be destroyed at the appropriate time under UCEM’s document retention and destruction policy
- Keys to any UCEM property or equipment should be unmarked and kept in a secure key store.

Please also refer to the Remote Working Policy for further detailed advice on remote working and the use of laptops, mobile phones, tablets and memory sticks.

Communications

Many of the breaches of data security reported to the Information Commissioner involve issues with email and all staff must have regard to the following:

- Consider whether the content of email should be encrypted or password protected

- Some email software "suggests" addresses as you type. Check which is the correct one.
- Use blind copy, not carbon copy, if you do not want recipient's email revealed to others
- Be very careful with groups on email. Check the current listing before using. Does everyone in the group need to see the email? Is it appropriate?
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. Check the security of the recipient and whether there is a data sharing agreement in place. If necessary, agree a different way to send the information
- Be wary of long email chains. There might be people at the beginning of the chain who should not see the email you are sending.
- Be aware that email is an open system, and emails may have to be disclosed because of a Subject Access Request. Do not send an email which you would not be happy to have read out in open court.

Storage

All staff are responsible for keeping a record of their work in accordance with agreed procedures. Staff can make use of social media for work purposes but must ensure that anything they contribute which has continuing value to the organisation is added to the organisation's records. The boundaries between work and personal easily blur. If the communication relates to work it is corporate information which must be available to those who need that information. Emails sent, or received, from portable devices should be stored in the right place so those who need to see them can do so.

When a file is opened there should be a review, or destruction, date which will either be when the file is closed, or a set period after closure. Whether the file is manual, electronic, or both, a review or destruction date should be clearly noted on the file. For "general" or "management" files these can be reviewed two years from creation with an assumption that both paper and electronic copies will be destroyed unless there is a clear reason why it should be kept. For archive purposes only one copy of most management files is required and will be maintained by the Executive Support Team

Both electronic and paper files should be stored in systems allowing easy access to those who need to use those files. Files contain information that can be useful, possibly vital, for others to know. Equally files may contain sensitive personal data and should only be accessible to those who need to know. We have guidelines on storage of information and these should be followed

All files should be stored securely. For detail on secure storage electronically and the use of laptops, tablets, mobile phones and memory sticks please refer to the Remote Working Policy**.**

There is a document retention and destruction policy which should be complied with.

Appendix Five

Data security breach procedure

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can be about a breach of confidentiality, availability of data or integrity of data. All personal data breaches are security incidents. Not all security incidents are necessarily personal data breaches.

Examples of data breaches are:

- Data is sent to the wrong person or files are left in a public area.
- IT equipment is lost or stolen. Even if the information is encrypted a potential information security breach has occurred and needs to be investigated
- Paper records are lost or stolen.
- Data is destroyed when it should not be.
- Data is damaged in some manner.
- Mobile technology is lost or stolen

What to do first

On becoming aware of a data security breach, the IT support helpdesk must be informed immediately. They will then log the issue in the **Information Security Breach Log.**

As soon as IT Support have logged the breach they will attempt to contact the DPO as it is their responsibility to ensure that the breach is handled correctly.
If the breach is serious (see definition of serious below) then the DPO should be contacted immediately by phone or in person. If they cannot be contacted then attempts should be made to contact another Vice-Principal or Dean so that they are aware of the situation.

For a non-serious breach, so long as the DPO can be contacted within 24 hours there is no need to contact another Vice-Principal or Dean.

An information security breach will be classified as serious if there is a likely risk to individuals as a result of the breach. Examples of a serious breach are:

- Data has been disclosed due to malicious action (e.g. a hacker has gained access to information)
- Electronic data on a number of people (students or staff) has been lost and it is unencrypted
- Information on a number of people has been disclosed and the information contains more than a simple list of names
- Disability, health or banking information has been disclosed for any individual

Investigate breach

IT Support should immediately attempt to establish the nature/risk of breach, as not all breaches will be significant, by establishing the following:
1. What type of data is involved?

2. Who is the data controller? If UCEM has disclosed any information it is important, but if UCEM is not the data controller then this means other organisations will need to be informed

3. How sensitive is the data? – both in terms of the DPA and to the individuals.

4. What damage could be caused to individuals?

5. What data subjects have been affected?

6. How many data subjects have been affected?

7. What is the breach?

8. What systems are affected?

9. Where is the relevant information held?

10. Any third parties involved? E.g. other data controllers or data processors

11. Are there any wider consequences to consider? – for example physical safety

Containment

Once it is clear what has happened and what has been exposed then the first priority is one of containment. That is ensuring business continuity by deciding what immediate corrective action is required to close the breach. This should consider whether anything can be done to recover the loss and any steps to limit the damage. The actions taken will need to be documented.

Notification

We will notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those concerned directly.

If communicating the most appropriate method of communication should be selected (post, email, phone) which will be influenced by:

- Urgency/cost
- Quality of database – it is not possible to phone if no phone numbers exist
- Information to be provided – if forms are to be supplied the phone is not appropriate

The actual communication should contain the following:

- The nature of the breach including how and where it happened
- Name and contact details of the Data Protection Officer
- Likely consequences
- What data was involved
- The steps taken, or being taken, to mitigate any issues
- Steps data subject can take to avoid issues (e.g. resetting passwords)
- Links to/information on any further help available

Importantly it must be written in clear plain English and must be checked to ensure the communication is not going to compound the issue. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

A notifiable breach will be reported to the relevant supervisory authority **within 72 hours** of UCEM becoming aware of it. The DPA 2018 recognises that it will often be impossible to investigate a breach fully within that time-period and allows for the provision of information in phases. If the breach is sufficiently serious to warrant notification to the public, UCEM will do this without undue delay.

Record keeping and learning lessons

Throughout the process everything should be documented in the **Information Security Breach Report** for the particular incident. This is vital as the ICO will expect to see documentary evidence that an investigation has been carried out.

These reports should be stored in the Data Protection File for five years.

The **Information Security Breach Log** should be used to capture the top-level information and will be used as a summary and to ensure all actions have been closed.
The detail on the breach and the activities taken to resolve it should be recorded as the breach is investigated and resolved.

There is a naming convention – including folder, title, date and initials to help with audit trail. The DPO is responsible for this.

All Information Security Breach Reports will be presented to the Senior Leadership Team at their next available meeting.

Appendix Six

HESA Student Collection Notice

We are obliged to make this notice available to students as part of our own Data Protection Policy

Student and leaver surveys

Your contact details may be passed to survey contractors to carry out the National Student Survey (NSS) and surveys of student finances, on behalf of some of the organisations listed below under Purpose 1.

These organisations and their contractors will use your details only for that purpose, and will then delete them. About six months after you graduate, we may contact you to ask you to fill in the Higher Education Statistics Agency ('HESA') 'Destinations of Leavers from HE' questionnaire. You may also be contacted as part of an audit to check that we have undertaken this survey properly. We will not give your contact details to HESA. You may also be included in longitudinal surveys of leavers in the years after you graduate. If so, we will pass your contact details to the organisation that has been contracted to carry out that survey. That organisation will use your details only for that purpose, and will then delete them. If you do not want to take part in any of these surveys, please let us know.

Submission of your information to HESA

Every year we will send some of the information we hold about you to HESA ("your HESA information"). HESA is the official source of data about UK universities and higher education colleges (www.hesa.ac.uk). HESA collects, and is responsible for, the database in which your HESA information is stored. HESA will never provide information that identifies individual students. It deals only with statistical information. HESA is a registered charity and operates on a not-for-profit basis. HESA uses your HESA information itself for its own purposes. HESA also shares information from your HESA information with third parties. It may charge other organisations to whom it provides services and data. HESA's use of your HESA information may include linking information from it to other data, as described further below. All uses of HESA information must comply with the Data Protection Act 1998/ 2018

Sensitive information

If you give us information about your disability status, ethnicity, sexual orientation, gender reassignment or religion these may be included in your HESA information and used to assist with monitoring equality of opportunity and eliminating unlawful discrimination in accordance with the Equality Act. Some other sensitive information is used to enable research into the provision of fair access to higher education, for example, information as to whether you are a care leaver. If you are enrolled at a higher education provider in England regulated by the Higher Education Funding Council for England your HESA information will include details of any financial support you may receive from us. Your sensitive information will not be used to make decisions about you. Your HESA information (including linked data) is used for four broad purposes:

Purpose One - Public functions - Education statistics and data. Your HESA information is used by some organisations to help carry out public functions connected with education in the UK. These organisations are data controllers in common of your HESA information under the terms of the Data Protection Act (this link explains what this means ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/). Such organisations may include:

- Department for Business, Innovation and Skills

- Welsh Government
- Scottish Government
- Department for Employment and Learning, Northern Ireland
- Higher Education Funding Council for England
- Higher Education Funding Council for Wales
- Scottish Further and Higher Education Funding Council
- Department for Education
- Research Councils
- Education Funding Agency
- National College for Teaching and Leadership
- National Health Service
- General Medical Council
- Office for Fair Access
- Quality Assurance Agency for Higher Education and any successor bodies.

Other Uses - Your HESA information may also be used by some organisations who are also data controllers in common to help carry out public functions that are not connected with education. Such uses may include the following:

- Measurement of population levels and migration by the Office for National Statistics, National Records of Scotland and the Northern Ireland Statistics and Research Agency
- Monitoring of public expenditure by the National Audit Office
- Monitoring of the accuracy of electoral registers by Electoral Registration Officials.

Purpose 2 - Administrative uses

Your HESA information may be used to audit claims to public funding and student finance, and to detect and prevent fraud.

Previous study - if you are enrolled at an HE provider in England the Higher Education Funding Council for England (HEFCE) may share your previous education records with us, including information submitted by other institutions, to determine the nature of any prior higher education study, including your current qualifications. This may be used to make decisions about the fees you are required to pay, the support available to you or the availability of a place for you to study with us. Your HESA information will not be used to make decisions about you other than for those uses outlined under Purpose 2.

Purpose 3 - HESA publications

HESA uses your HESA information to produce and publish information and statistics. This includes some National Statistics publications (www.statisticsauthority.gov.uk/nationalstatistician/types-of-official-statistics) and online business intelligence and research services. HESA will take precautions to ensure that individuals are not identified from any information which is processed for Purpose 3.

Purpose 4 - Equal opportunity, research, journalism and other processing in which there is a legitimate interest

HESA and the other data controllers in common (see Purpose 1) may also supply information to third parties where there is a legitimate interest in doing so. Examples of use for this purpose include:

• Equal opportunities monitoring

• Research - This may be academic research, commercial research or other statistical research where this is in the public interest

• Journalism - Where the relevant publication would be in the public interest e.g. league tables

• Provision of information to students and prospective students

Users to whom information may be supplied for Purpose 4 include:

• Higher education sector bodies

• Higher education providers

• Academic researchers and students

• Commercial organisations (e.g. recruitment firms, housing providers, graduate employers)

• Unions

• Non-governmental organisations and charities

• Local, regional and national government bodies

• Journalists

Information supplied by HESA to third parties within Purpose 4 is supplied under contracts which require that individuals shall not be identified from the supplied information.

HESA student information may be linked to school and/or further education college information and supplied to researchers. A copy of the Agreement for the supply of linked data about pupils from schools in England is available at www.gov.uk/government/collections/national-pupil-database

Linking of information in the HESA record

As indicated above, where HESA and organisations covered by Purpose 1 use HESA information this may include linking HESA information to other information for example:

• UCAS data

• National Student Survey data

• School and Further Education data

• Student Loans Company data

• Qualification Awarding Bodies data

• Tax, Benefits, and Employment data.

Where HESA provides information from your HESA information to third parties under Purpose 4, the permitted uses of the information by a third party may include linking HESA information to other information held by the third party. Permission for such use is considered on a case by case basis. It is only given where the linking is for the purposes outlined in Purpose 4 and subject to the requirement not to carry out linking to identify individuals.

Destinations information for schools and colleges

If you attended a school or college in England linked data may be disclosed to the last school or college you attended (or its successor body) to enable them to assess the outcomes of secondary and further education.

About the HESA student collection notice

The HESA Student Collection Notice is regularly reviewed. The most up to date version can be found at www.hesa.ac.uk/fpn. Minor updates to the Student Collection Notice (including organisation name changes and clarification of previously specified purposes) may be made at any time. Major updates (such as a new purpose or administrative use) will be made no more than once per year.

Your rights under the Data Protection Act 1998/2018

You have rights of access to the information HESA holds about you. You will have to pay a small fee for this under the 1998 Act but from May 2018 this will not be necessary. For further information about data protection and your HESA information please see the HESA website, *Data Protection* [online]. Further information is available **http://www.hesa.ac.uk/dataprot** or **email data.protection@hesa.ac.uk.**

Appendix Seven / F

Education and Skills Funding Agency (ESFA) Privacy Notice

ILR Specification 2017 to 2018 - Appendix F – Privacy Notice

Appendix F - Privacy Notice 2017 to 2018

Version 1 - Published 28 April 2017

Training providers should ensure that all learners have seen this privacy notice as part of their enrolment processes.

How We Use Your Personal Information

This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 1998, the DfE is the data controller for personal data processed by the ESFA.

Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR).

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998.

The English European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.

You can opt out of contact for other purposes by ticking any of the following boxes if you do not wish to be contacted:

- ☐ About courses or learning opportunities.
- ☐ For surveys and research.

- ☐ By post.
- ☐ By phone.
- ☐ By e-mail.

Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:

https://www.gov.uk/government/publications/esfa-privacy-notice