Queen Margaret University

EDINBURGH

Data Protection Policy

Policy Summary:	This policy sets out your obligations when processing the personal information of others in the course of your employment
Policy Owner:	Human Resources
Approved By:	GDPR Steering Group
Consultation Completed:	TBC
Equality Impact Assessed:	TBC
Date of Issue:	May 2018
Review Period:	Annually or as required by legislation
Last reviewed:	N/A

DATA PROTECTION POLICY

1 Aim of this policy

Queen Margaret University is committed to protecting personal information in line with our obligations under data protection law.

This policy sets out your obligations when processing the personal information of others in the course of your work for us. It is essential that you read this policy and comply with it – non-compliance may be a disciplinary offence.

Your compliance with this policy will help us to meet our objectives of:

- Protecting individuals whose personal information we process;
- Maintaining confidence in our organisation and our business reputation; and
- Complying with our legal obligations – if our organisation fails to comply with data protection law, this can lead to significant sanctions, including substantial fines.

2 Who does this policy apply to?

This policy applies to all employees, workers and contractors.

3 Does this policy form part of my contract?

This policy does not form part of your contract except to the extent that it imposes obligations on you. We may amend this policy at any time and may vary it as appropriate to a particular case.

4 Confidentiality of policy

This policy is an internal, confidential document. You must not share it with third parties, clients or regulators without prior authorisation from the Data Protection Officer.

5 Data protection officer/Data protection queries

We have appointed a data protection officer. If you have any questions about this policy or your data protection obligations please contact Irene Hynd, University Secretary (May/June 2018) and Lorraine Kerr, Legal Adviser and DPO (from July 2018).

6 Meaning of terms in this policy

In this policy, the following terms have the following meanings:

Term	Meaning
Personal information	Information about a living individual from which they can be identified (or from which they can be identified along with other information we hold or can reasonably access). This information can be stored in any media (eg. paper or a computer database). Some examples are: • Personal contact details, such as name, address, email, telephone number. • Date of birth. • Bank account details. • Opinion about a person's actions or behaviour, for example, expressed in an email or interview notes. Personal information can relate to, for example, past or present employees, workers, contractors, customers, clients, suppliers, shareholders, website users or members of the public. Personal information does not include data where the identity has been removed (anonymous data).
Special categories of personal information	Information about an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions, offences or alleged offences; genetic data; or biometric data for the purpose of uniquely identifying an individual.
Processing	Any activity that involves using personal information. This includes collecting personal information, recording it, storing it, retrieving it, using it, amending it, disclosing it, destroying it, and transferring it to third parties.

7 Data protection principles

When processing personal information, we must adhere to the following data protection principles. Personal information must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Not kept in a form which permits identification of individuals for longer than necessary, in relation to the purposes for which it is processed;
- Kept secure, and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

8 Your obligation to comply with privacy notices and other policies

In the course of your work for us, you must only process personal information in accordance with:

- Our Employee Privacy Notice, as regards the personal information of our employees.
- Our Student Privacy Notice, as regards the personal information of students.
- Our Alumni Privacy Notice, as regards the personal information of former students who have registered with our Development Office; and
- Any relevant policies, guidelines and procedures that we put in place.

You must ensure that you have read and understood the privacy notices and any relevant policies, guidelines and procedures. Contact the Data Protection Officer if you are unsure about any aspect of these.

You must contact the Data Protection Officer immediately if you are unsure whether particular processing of personal information is within the terms of the relevant

privacy notice, or you are otherwise unsure as to whether we have a lawful basis for processing particular personal information.

9 Data protection: your other obligations

In the course of your work for us, you must ensure that:

Necessary, relevant, accurate

- You only access and process personal information that is necessary to perform your work. You must not access or process personal information for any reason unrelated to your work.
- You only collect personal information that we actually need – it must be relevant, given the purpose for its collection. Do not collect excessive personal information.
- As far as possible, the personal information you process is accurate and up to date.
- You maintain accurate records of your work and the personal information that you process.

Appropriate language

- You use appropriate language if you record an opinion about someone (for example, in an email) bearing in mind that they may be entitled to see this.

Don't mislead

- You don't mislead anyone as to how their personal information may be used.

Security: general

- You keep personal information secure and perform your work in such a way as to protect the personal information that we hold. In particular, you must comply with all policies, guidelines and procedures that we put in place to secure personal information (including the use of any technology). You must take particular care in protecting special categories of personal information from loss or unauthorised access, use or disclosure.
- You do not attempt to circumvent the safeguards we use to protect personal information (including administrative, physical and technical safeguards).

- Unless our policies specifically allow you to do otherwise, you store all personal information in our systems or, for paper records, on our premises, and you do not remove personal information from our premises (in electronic or paper format) or store personal information elsewhere (for example, on a computer, laptop or mobile phone not provided by us).

- If you have permission to remove personal information from our premises, when outside of our premises, you do not leave any paperwork containing personal information, or any device or material on which personal information is stored, unattended at any time.

- You keep all passwords secure and do not reveal them to anyone else.

- You only dispose of paperwork containing personal information in the confidential waste bins provided on our premises.

- You do not create unnecessary copies of personal information.

Security: communications

- You check that the addresses are correct on letters, emails or other communications you are sending that contain personal information, and that any attachments or enclosures are correct. Take particular care to check email addresses when using a predictive (auto-complete) email address function, or if an email is going to multiple addressees.

- When communicating with someone by email for the first time, you send a test message to establish that you have the correct email address before sending any personal information.

- You consider whether the means you are using to communicate personal information is appropriate, taking account of the sensitivity of the content.

- You do not use your personal email address for work purposes.

- You do not discuss or reveal personal information which relates to workplace matters in a public setting where it may be seen or overheard.

Sharing personal information

- You comply with any policies, guidelines or procedures relating to the sharing of personal information.

- You only share personal information with another of our employees, workers or contractors, or with one of our agents or representatives, if that person has a work-related need to know the information.

- You only share personal information with third parties (including, for example, our service providers) if:

    - they have a need to know the personal information (for example, in order to provide services to us);

    - the relevant privacy notice gives notice that the personal information may be shared with that third party; and

    - you are satisfied that the third party will comply with the data protection principles at clause 7 above, in particular that the personal information will be kept secure.

Training

- You have undergone our mandatory GDPR e-learning training and, if you are a line manager, that your team has undertaken the GDPR e-learning module

No longer than necessary

- If you are responsible for the deletion or anonymization of personal information, this is done in accordance with any relevant privacy notice or policy. We must not keep personal information for longer than necessary.

Personal information collected indirectly (eg. from third parties)

- If you are responsible for collecting the personal information of any individual indirectly (i.e. not from the individual themselves but, for example, from a third party or publicly available source) you ensure that the individual receives the relevant privacy notice either:

    - within a reasonable period after you collect the information (maximum one month), unless this would involve disproportionate effort; or

    - if you use the personal information to communicate with the individual before then, when the first communication with them takes place (at the latest); or

- if you are disclosing the personal information to someone else, before this happens.

- You contact the Data Protection Officer immediately if you are concerned that personal information provided to you by a third party has not been collected in accordance with the data protection principles at clause 7 above.

Personal information you acquire in error

- You inform the Data Protection Officer immediately if you acquire any personal information in error.

10 Notify the Data Protection Officer of certain activities

It may be necessary for Data Protection Officer to carry out a 'data protection impact assessment' before you undertake certain activities that involve processing personal information.

A 'data protection impact assessment' will consider the impact of the activities; identify privacy risks and steps to minimise those risks; and evaluate whether the activities are permitted by data protection law.

As such, you should seek advice from the Data Protection Officer so they can advise whether a data protection impact assessment is required:

- Process new types of personal information i.e. personal information which has not been collected before.

- Process personal information in a new or significantly different way, including via the use of new technologies.

- Use personal information for a purpose other than that for which it was collected.

- Enter a contract with a third party that involves disclosing or sharing personal information.

- Any new or significantly different use of automated processing of personal information to evaluate an individual, for example to analyse or predict an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- Any new or significantly different use of automated decision-making i.e. where a decision is made on a solely automated basis without meaningful human involvement, and it has a significant effect on individuals.

- Any new or significantly different large scale processing of special categories of personal information; or large scale, systematic monitoring of a publicly accessible area. Whether processing is 'large scale' will depend on, for example, the number of individuals, volume of data, range of data, duration of processing, or geographical extent – if you are in any doubt as to whether processing is large scale, contact the Data Protection Officer.

- Implement significant changes to systems or the business (including new or different technology) which involve processing personal information.

- Any new direct marketing activity (including electronic marketing by email, telephone, fax or text message) that is not clearly authorised by the Director of Marketing and Communication.

- Transmit or send personal information to, or view or access personal information in, a country outside of the European Economic Area (EEA), where this has not been previously authorised by the Data Protection Officer or in line with the University Data Protection Policy. The EEA is the 28 countries in the European Union, along with Iceland, Liechtenstein and Norway.

You must comply with any directions from [the data protection [officer/manager]] in relation to the above, and the terms of any data protection impact assessment.

11 Individuals' rights: what you need to do

Individuals may have certain rights as regards their personal information, including to:

- Receive certain information about our processing;

- Request access to their personal information that we hold (often known as a 'subject access request');

- Request transfer, correction, deletion, restriction of processing;

- Object to processing (including where this is for direct marketing);

- Request a copy of an agreement transferring personal information outside of the European Economic Area;
- Object to decisions based solely on automated processing, including profiling;
- Be notified of a personal information breach;
- Complain to the Information Commissioner; or
- Withdraw their consent to processing (if we process their personal information on the basis of their consent).

If you receive any communication that appears to relate to these rights, you must contact the Data Protection Officer **immediately**. Do not respond to the communication or attempt to deal with it without input from the Data Protection Officer.

12 Reporting a personal information breach

A personal information breach means anything that compromises the security, confidentiality, integrity or availability of personal information or the safeguards that protect it. This could include where personal information is lost, or where it is accessed, disclosed or acquired without authority.

If you know or suspect that there has been a personal information breach, you must preserve all evidence and **immediately** contact the Data Protection Officer. You must make this contact immediately (even outside of business hours and at nights or weekends) in order to:

- reduce the risk of damage to any affected individuals and our business; and
- allow us to comply with any obligation to notify the Information Commissioner (the UK supervisory authority for data protection) or the individuals affected.

Our procedure for dealing with suspected personal information breaches is set out in our Personal Information Breach Policy

13 Breaches of this policy

If you think you may have breached this policy, please speak to your line manager or the Data Protection Officer as soon as possible. Quick action can be crucial in mitigating the effects of a breach.

Breaches of this policy may be dealt with under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to dismissal without notice.