DATA PROTECTION POLICY

Index

Version number	Version 1.0
Author/originator	Head of Information Assurance
Review Date	1st May 2019
Ratified/authorised by	VCAG
Issue date	25th May 2018
Person responsible for the document	Head of Information Assurance

1. Purpose and Scope

1.1 This Policy sets out the responsibilities of the University, its staff and its students to comply fully with the provisions of data protection legislation and the General Data Protection Regulation ('the GDPR'). It is accompanied by a list and links to other, associated policies and a Data Protection Guidance Handbook which provides information and guidance on different aspects of data protection and data security. This policy, its associated policies and the Guidance Handbook form the framework from which staff and students should operate to ensure compliance with data protection legislation.

1.2 This Policy applies to all staff and students, and all items of personal data that are created, collected, stored and/or processed through any activity of the University of Worcester and its subsidiaries. Any deliberate breach of this policy may lead to disciplinary action being taken, access to University facilities being withdrawn, or even criminal prosecution.

2. General

2.1 In undertaking the business of the University of Worcester large amounts of data on a variety of data subjects including students (both potential, current and former), staff, customers/suppliers and members of the public are created, gathered, stored and processed.

2.2 Some of this data we will be other people's personal and/or special category data i.e. concerning a data subject's racial or ethnic origin, political opinions, religious belief, trade union activities, physical or mental health or sexual life.

2.3 Recording and use of personal data continues to increase, so it is important that every member of staff understands the law that exists in relation to data protection and staff responsibilities in ensuring that data is secured and protected in line with the law.

2.4 Data protection is an important part of the University's overall information security arrangements. All information must be handled safely and securely according to the Information Classification and Handling Table. In addition to good practice, some data sets are subject to external legislation and it is vital that staff recognise both categories in their handling of University information and data.

2.5 The GDPR applies to all data relating to, and descriptive of, living individuals defined in the GDPR as 'personal data'. Individuals are referred to as 'data subjects'. For further definitions of terms used please see the glossary in Section 1 of the Data Protection Guidance Handbook.

2.6 The GDPR places obligations on the University and the way it handles personal data. In turn the staff and students of the University have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a lawful basis for processing it and have provided information to the individuals concerned about how and why their information is processed(i.e. a privacy notice). In the majority of cases the lawful basis for processing is likely to be due to a contract between the organisation and individual (e.g. employment or education contract), a statutory legal

obligation (e.g. HMRC requirements) or the individual's consent. There are restrictions on what is done with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

2.7 The University of Worcester is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

2.8 The University is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. For more information about these records - see Section 9.

3. Data Protection Principles

3.1 The University is required to adhere to the six principles of data protection as laid out in the GDPR. This means that information must be collected and used fairly, stored safely and not disclosed to any other person or organisation unlawfully.

3.2 The six principles are as follows, the names of each principal is indicated in the brackets:

i) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')

ii) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historic research or statistical purposes is permissible ('purpose limitation')

iii) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation')

iv) Personal data shall be accurate and where necessary kept up to date ('accuracy')

v) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation')

vi) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

3.3 In addition, the GDPR states that the controller shall be responsible for, and be able to demonstrate compliance with the above principles ('accountability').

4. Definitions

4.1 'Personal data' is information about a living individual, who can be identified, directly or indirectly, from that data. This data may include an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identify of that individual. These may include data specifically classed as 'special categories' of personal

data which include particularly sensitive data such as health details, racial or ethnic origin, religious beliefs, sexual life, trade union membership. More information is available in Section 2 of the Data Protection Guidance Handbook.

4.2 'Processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

4.3 The University is the 'data controller' and remains responsible for the control of the personal data it collects even if that data is later passed on to another organisation or is stored on systems or devices owned by other organisation or individuals (including devices personally owned by members of staff).

4.4 'Data protection impact assessments' may be required by staff developing new projects or processes, or revising existing processes, which include the processing of personal data. Additional information is available in Section 12 of the Data Protection Guidance Handbook.

4.5 The University's 'Data Protection Officer' is the Head of Information Assurance.

Further definitions are set out in Section 1 of the Data Protection Guidance Handbook.

5. Data Security

5.1 All University users of personal data must ensure that all personal data they hold, whether paper or electronic, is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Data Security should be undertaken in line with the Information Security Policy and Information Classification and Handling Table.

6. Data Retention

6.1 Individuals areas within the University are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on the University's Document Retention Schedule.

6.2 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Paper records should be disposed of via the University's confidential waste collection service and electronic records should be permanently deleted.

6.3 If data is fully anonymised then there are no time limits on storage from a data protection point of view.

7. Conditions of Processing and Consent

7.1 In order for it to be legal and appropriate for the University to process personal data at least one of the following conditions must be met (Article 6):

a) The data subject has given his or her consent ('consent')

b) The processing is necessary for the performance of a contract ('contract')e.g. educational or employment contract

c) The processing is necessary for compliance with a legal obligation ('legal')

d) The processing is necessary to protect someone's vital interests ('vital interests') e.g. life or death situation

e) The processing is necessary for the performance of a task carried out in the public interest ('public interest')

f) The processing is necessary for the legitimate interests of the controller and does not interfere with the rights and freedoms of the data subject. ('legitimate interests'). This condition cannot be used by public authorities in performance of their public tasks.

All processing of personal data carried out by the University must meet one or more of the conditions above. In most cases the personal data processed relating to students will be for the delivery of their educational contract, and, in the case of staff in relation to their employment contract. Consent should only be relied on in particular circumstances (see 7.4 and 7.5 below)

7.2 In addition the processing of 'special categories' of personal data requires additional, and more stringent, conditions to be met in accordance with Article 9 of the GDPR (Section 2 of the Data Protection Guidance Handbook). Special categories, previously called sensitive personal data, includes:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

The processing of this data requires an additional lawful basis which in most cases will be consent. Further advice can be sought from the Data Protection Officer.

7.3 Under the GDPR universities are classed as public authorities and therefore the use of the 'legitimate interests' condition is not possible in terms of the University of Worcester's core activities (public tasks). It may be possible to use 'legitimate interests' for processing; advice should be sought from the University's Data Protection Officer.

7.4 Public authorities are not encouraged to use consent for core activities due to the imbalance in the relationship between the controller and data subject. In these cases it is unlikely that consent could be deemed to be freely given. Therefore where possible the University should

identify alternative conditions for processing which would normally be 'contract' or 'legal', in these cases the relevant part of the contract or legal obligation should be identified.

7.5 'Consent' is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent. Anyone who has provided consent has the right to revoke their consent at any time. Further information about obtaining consent can be found in Section 5 of the Data Protection Guidance Handbook.

8. Privacy Notices

8.1 Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with a 'Privacy Notice' to let them know what it does with their personal data (the main Privacy Notices for the University are the Student Privacy Notice, Staff Privacy Notice and the Research Participants, Supporters and Visitors Privacy Notice.

8.2 Privacy notices are published on the University website and are therefore available to staff, students and visitors from their first point of contact with the University. Any processing of staff or student data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided. Further information about Privacy Notices can be found in Section 5 of the Data Protection Guidance Handbook.

8.3 When personal data is being collected the data subject's attention should be drawn to the relevant privacy notice either through a link and text on the collection notice or by sharing a link in a follow up email. Standard text is available at 'Guidance on writing Privacy Notices' .

9. Records of Processing Activities

9.1 As a Data Controller the University is required to maintain a record of processing activities which covers all processing of personal data carried out by the University. Amongst other things this record contains details of why personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. The University has three Records of Processing activities:

- Staff data (including job applicants, previous staff, honorary, emeritus and visiting staff)
- Student data (including applicants and alumni)
- Visitors (including: visitors to the University, users of University facilities and attendees at University organised events held elsewhere).

The Records of Processing can be accessed via this weblink

9.2 Staff embarking on new activities involving the use of personal data and that is not covered by one of the existing records of processing activities should inform the Data Protection Officer before starting the new activity.

10. Children

10.1 Under the GDPR, the following restrictions apply to the processing of personal information relating to children:

- Online services offered directly to children require parental consent unless they are a preventive or counselling service.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

10.2 If you are relying on consent as the lawful basis for processing personal data children aged 13 or over are able to provide their own consent (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). For children under this age you need consent from whoever holds parental responsibility for the child.

10.3 Privacy Notices should be clear so children are able to understand what will happen to their personal data and what rights they have. Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

10.4 The Data Protection Officer should be informed if any of the above activities are being contemplated.

11. Personal Data Breach

11.1 Any potential data breach needs to be reported immediately to allow the University to take mitigating action and comply with the requirement to report most data breaches to the Information Commissioner's Office within 72 hours of the breach being discovered. Staff should make themselves familiar with Personal Data Breach Notification Procedure and associated information on the Data Protection webpages.

12. Subject Access Requests

12.1 The GDPR gives data subjects the right to access personal information held about them by the University. The purpose of the subject access request is to allow individuals to confirm the accuracy of their personal data and check the lawfulness of processing which in turn allows them to exercise their rights of correction or objection if necessary. Individuals can request to see any information that the University holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

12.2 The University must respond to all requests for personal information normally within one calendar month and information will normally be provided free of charge, provided the request is reasonable.

12.3 References are disclosable to the person about whom they are written under the subject access provisions of the GDPR. This includes references received by the University from external sources and confidential references given and received internally e.g. as part of advancement and promotions procedures. There is an exemption from disclosure for references written by University staff and sent externally, however these references would still be accessible to the applicant from the organisation to which the references was sent.

12.4 The University is not required to disclose examination scripts, however students are entitled to access any marks or comment annotated on the script. Students are entitled to their marks for both coursework and examinations.

12.5 For information about making a subject access request see Requests for Personal Data. Further information and guidance about handling subject access requests can be found in Section 7 of the Data Protection Guidance Handbook.

13. Individual's Rights

13.1 Data subjects have a number of other rights, aside from the right to see information the organisation holds on them. These include:

- **Right to object** - Data subjects have the right to object to specific types of processing which includes processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right (see Section 18 on Direct Marketing). Online services must offer an automated method of objecting. In some cases there may be an exemption to this right for research or statistical purposes.
- **Right to be forgotten (erasure)** - Individuals have the right to have their data erased in certain situations such as where the data is no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example about accuracy) are resolved or the processing is potentially unlawful.
- **Rights in relation to automated decision making and profiling** - This right relates to automated decisions or profiling that could significantly affect an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision making based on sensitive data can only be done with explicit consent.
- **Right to Rectification** - The right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data is incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.

- **Right to Portability** - the data subject has the right to request that information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (i.e. not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

The availability of rights largely depends on the legal justification for processing.

13.2 Any requests made to invoke any of the rights above must be dealt with promptly and within one month of receiving the request. Members of staff should consult the Data Protection Officer if any such requests are received.

14. Data Sharing with Third Parties

14.1 Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the University.

14.2 Staff who receive requests for personal information from third parties such as relatives, police, local councils etc should consult Section 8 of the Data Protection Guidance Handbook on Requests for Personal Information from Third Parties.

14.3 As a general rule, personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible:

- Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned (see Section 3)
- It must meet one of the conditions of processing (see Section 7). Legitimate reasons for transferring data would include:
  - That it was a legal requirement
  - It is necessary for the official core business of the University
- If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided (see Section 5 on Consent and Privacy Notices in Data Protection Guidance Handbook)
- The University is satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.
- Where a third party is processing personal data on behalf of the University a written contract must be in place. A contract is also advisable when data is being shared for reasons other than data processing so the University has assurances that GDPR requirements are being met

14.4 Staff should consult the Data Protection Officer if they are entering into a new contract that involves the sharing or processing of personal data.

15. Transfers of Personal Data Outside the EU

15.1 Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. In many cases the University will require consent of the data subjects before personal information can be transferred out of the EU.

15.2 Information published on the internet must be considered to be an export of data outside the EU. This covers data stored in the cloud unless the service provider explicitly guarantees data storage only takes place within the EU.

15.3 The Information Commissioner's Office Guidance on the use of Cloud Computing should be consulted before any use of external computing resources of services via a network which may involve personal data.

15.4 Staff involved in transferring personal data to other countries should consult Section 10 of the Data Protection Guidance Handbook and advise the Data Protection Officer.

16. Data Protection Impact Assessments and Data Protection by Design

16.1 Under the GDPR the University has an obligation to consider the impact on individual's privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

16.2 It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. The GDPR imposes a specific 'privacy by design' requirement, emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an afterthought.

16.3 For some projects the GDPR **requires** that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include:

- those involving processing of large amounts of personal data;
- where there is automatic processing/profiling;
- processing of special categories of personal data;
- or monitoring or publicly assessable areas (i.e. CCTV).

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. Information about when and how to carry out a DPIA can be found in Section 12 of the Data Protection Guidance Handbook.

17. Research

17.1 Data collected for the purposes of research are covered by the GDPR. It is important that staff collecting data for the purpose of research or consultancy incorporate an appropriate form of consent on any data collection form.

17.2 Further information and guidance on data protection and research is provided in Researcher's Guide to the Data Protection Act (available from the Research Office).

18 Direct Marketing

18.1 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing materials that is directed to individuals e.g mail shots for fund raising, advertising courses etc. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. The University must cease direct marketing activity if an individual requests the marketing to stop.

18.2 Direct marketing must also comply with the Privacy and Electronic Communication (EC Directive) Regulations 2003 which covers marketing via telephone, text and email. For more information about direct marketing please see Section 14 of the Data Protection Guidance Handbook.

19. Impact of Non-Compliance

19.1 All staff and students of the University are required to comply with this Data Protection Policy, its supporting policies and guidance and the requirements specified in the GDPR. Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the University i.e. for their own purposes, which are outside the legitimate purposes of the University.

19.2 The University could be fined for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement. Further information about the fines are in Section 15 of the Data Protection Guidance Handbook.

20. University Contacts

20.1 The University's named Data Protection Officer is Helen Johnstone, Head of Information Assurance.

20.2 In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to infoassurance@worc.ac.uk.

21. Other relevant documentation

Personal Data Breach Incident Management Procedure

Data Protection Guidance Handbook

Information Security Policy

IT Regulations