DATA PROTECTION POLICY

Contents

1. Purpose and Scope

1.1 This Policy sets out the responsibilities of all those who process personal data in respect of which the University is the data controller, e.g. staff and volunteers, to ensure compliance with the provisions of the UK data protection legislation, including but not limited to the UK General Data Protection Regulation (the 'UK GDPR') and the Data Protection Act 2018 (the 'DPA 2018'). This Policy together with the guidance on the Information Assurance webpage form the framework from which staff and (where applicable) students should operate to ensure that personal data is processed in accordance with the data protection legislation.

1.2 This Policy applies to all items of personal data that are processed through any activity of the University of Worcester (the 'University') and its subsidiaries. All staff and others processing personal data on the University's behalf must read and comply with it. Breaches of this Policy may lead to disciplinary or other appropriate action being taken.

2. General

2.1 In undertaking the business of the University large amounts of personal data on a variety of data subjects, including applicants, students (both current and former), staff, customers/suppliers, visitors, research participants and members of the public, are created, gathered, stored and processed for a variety of specified and lawful purposes, set out in privacy notices issued when the personal data is collected.

2.2 In order to comply with the data protection legislation, personal data must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

2.3 Responsibility for complying with data protection legislation extends to all staff and anyone else who process personal data on the University's behalf. Training will be provided to staff upon the commencement of their employment with periodic opportunities for refresher training thereafter. The Information Governance Officer is on hand to assist staff with day-to-day queries which cannot be answered by reading the guidance documents on the Information Assurance webpage.

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 and Document Retention Schedule. In addition to good practice, some data sets are subject to statutory retention or legal limitation periods and it is vital that staff observe these in their handling of University information and data.

2.5 The UK GDPR places obligations on the University and the way it handles personal data. 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 UK or using it for direct marketing.

2.6 The UK GDPR covers all personal data processed by the University, irrespective of whether the data is held by individual members of staff in their own separate files, paper or electronic,

(including those held outside the University campus e.g. by staff working at home or at partner institutions) or in Departmental records or centrally by the University.

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

3. Data Protection Principles

3.1 The University is required to adhere to the six principles of data protection as laid out in the UK 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 in a form which permits individuals to be identified for longer than is necessary for that purpose ('storage limitation'); and

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, personal data should not be transferred to another country outside the UK without appropriate safeguards being in place.

3.4 The UK GDPR states that the controller shall be responsible for, and be able to demonstrate compliance with the above principles ('accountability').

4. Definitions

- **Consent** - of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes buy which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- **Data Controller** - A 'data controller' is the person/organisation that determines when, why and how to process personal data. The University is the data controller of all the personal data we process for our own purpose. The University 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).

- **Data Protection Legislation** – All applicable data protection and privacy legislation in the UK to include the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2426/2003*) as amended and all applicable laws and regulations relating to the processing of the Personal Data and privacy, including where applicable the guidance and codes of practice issued by the UK Information Commissioner or any other national data protection authority, and the equivalent of any of the foregoing in any relevant jurisdiction

- **Personal Data** - is information about a living individual (the data subject) who is identifiable from that information or who could be identified from that information combined with other data which the University either holds or is likely to obtain. This includes names, contact details, photographs, salary, attendance records, student marks, sickness absence, leave, dates of birth, marital status, personal email address, online identifiers, IP addresses etc. Furthermore, any expression of opinion or any intentions regarding a person are also personal data.

- **Special Category Data -** The UK GDPR separately defines 'special categories of personal data' which relates to the following:
    - the racial or ethnic origin of the data subject;
    - their political opinions;
    - their religious or philosophical beliefs;
    - whether they are a member of a trade union;
    - their genetic data;
    - biometric data used to uniquely identify them;
    - their physical or mental health or condition; or
    - their sex life or sexual orientation.

- **Personal data relating to criminal convictions and offences** means personal data relating to criminal offences committed by an individual and offences alleged to have been committed, including proceedings for offences/alleged offences and the disposal of such proceedings, including sentencing.

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

- **Processor** - organisation, person or other body which processes personal data on behalf of the controller

- **Profiling** - automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.

- **Third party** - organisation, person or other body, other than the data subject, controller (and its employees) or processor

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 Individual 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, i.e. it is purely statistical data which does not include the student or staff identification number then there are no time limits on storage from a data protection point of view as this is no-longer 'personal data' – data which identifies an individual.

7. Lawful basis for Processing

7.1 In order for it to be legal and appropriate for the University to process personal data at least one of the following lawful bases must apply as set out in (Article 6) UK GDPR:

a) The data subject has given his or her consent (i.e. where the data subject has genuine choice and control) ('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 University as controller or of a third party except where those interests are overridden by 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 if there is no other relevant lawful

basis and in particular should be sought to process video or photographic images of an individual for promotional purposes, or when processing special category data as detailed at 7.2. below.

7.2 In addition to complying with one of the above legal bases, the processing of 'special categories' of personal data requires additional, and more stringent, conditions to be met in accordance with Article 9 of the UK GDPR. As required under Schedule 2, Part 4 of the Data Protection Act 2018 how the University protects Special Categories of Personal Data is set out in the Data Protection – Special Category and Criminals Convictions Data Policy

In the context of the University this would most often be:

- the individual has given their explicit consent(by means of a clear written statement);
- the special category data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law;
- the processing is necessary to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- the special category data has already been made manifestly public by the individual;
- the special category data needs to be processed for reasons of substantial public interest as defined by the DPA 2018, Schedule 1, Part 2 (e.g. safeguarding, preventing/detecting unlawful acts);
- the processing is required for occupational health, absence management or the provision of health or social care services or treatment; and
- the special category data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

7.3 For personal data relating to criminal convictions and offences, the University must comply with one of the lawful bases as set out above in 7.1 in relation to non-special category personal data and also meet one of the conditions specific to criminal convictions personal data as set out in the DPA 2018, Schedule 1. The DPA 2018, Schedule 1 conditions are similar to those that apply to special category data, including the substantial interest conditions provided by the DPA 2018, Schedule 1, Part 2.

Further advice can be sought from the Information Governance Officer.

7.4 Under the UK GDPR universities are classed as public authorities and therefore the use of the 'legitimate interests' legal basis is not possible in terms of the University's core activities (public tasks). It may be possible to use 'legitimate interests' for processing in other cases though; advice should be sought from the University's Information Governance Officer.

7.5 In relation to the personal data already processed by the University, we have documented the decision about what lawful basis we are relying upon to do so in our 'Records of Processing'. Staff may find it helpful to refer to these records in the first instance when considering a lawful basis for processing new data. If there are no relevant categories already within the Records of the Processing, advice should be sought from the University's Information Governance Officer.

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). These are published on the University website and are therefore available to staff, students and visitors from their first point of contact with the University.

8.2 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 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 UK. 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); and
- 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 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 UK 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. 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 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.

11.2 In accordance with the Personal Data Breach Notification Procedure linked above, Data breaches should be reported to infoassurance@worc.ac.uk. The form at the end of the Personal Data Breach Incident Management Procedure should be completed and returned as soon as possible after the incident.

12. Subject Access Requests

12.1 The UK 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 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, though a different time limit for compliance applies i.e. where the request is submitted before the results have been announced, a copy must be provided within 40 days of the announcement or within five months of the request, whichever is sooner.

12.4 For further information about subject access requests see Requests for Personal Data. You should pass any subject access request that you receive immediately to infoassurance@worc.ac.uk.

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 withdraw consent** – where processing is based on the data subject's consent, data subjects have the right to withdraw their consent that processing at any time. Consent should therefore only be relied on if there is no other lawful basis of processing.
- **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 19 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 limited circumstances, 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 Information Governance Officer if any such requests are received.

13.3 Data subjects also have the right to:

- be notified of a personal data breach (in certain circumstances e.g. where the breach poses a serious risk);
- make a complaint to the ICO; and
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

14. Requests for Personal Data from Third Parties (including the police and relatives)

14.1 The University often receives requests for the personal information on its students and staff from third parties. This section is intended to provide advice to staff on how such requests should be handled to ensure compliance with GDPR.

14.2 The University tells students, staff and visitors how their information will be used, and in what circumstances and to whom it may be disclosed in its Privacy Notices.

14.3 There are some third parties that can require disclosure of personal data, examples of these are in the table below:

Third Party	**Authorisation for Disclosure**
UK Funding Councils e.g. OfS, SFC and their agents e.g. QAA, HESA	Further and Higher Education Act 1992, s 79
Officers of the Department of Works and Pensions and Local Authorities	Social Security Administration Act 1992; s110A, a109B and s109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013, s3
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1998
Environment Agency	Agency Regulations – specific ones to be quoted
Child Support Agency (CSA)	Child Support (Information, Evidence and Disclosure) Regulations 1992
Inland Revenue	Taxes Management Act 1970
Police Officers	With a Court Order – see 14.9 for further advice
Regulatory bodies e.g. NMC; HCPC	Regulations made under the statute that created the particular body
Electoral Registration Officers	Representation of the People Regulations 2001, Regulation 23.
Other third parties	Request that they provide evidence of any statutory power to require disclosure, failing which disclosure may only be lawful, with a Court Order.

The University should not process personal information of individuals in ways that are not covered by our Privacy Notices, or where there is a legal requirement, without explicit consent.

As a general rule you should never disclose personal data to anyone other than an employee of the University with a legitimate work interest in the information, without consent or unless there is a clear legal obligation to do so. Advice should be sought from the Information Governance Officer.

14.4 How to handle common types of third-party request

14.4.1 Requests for references or confirming qualifications

Requests for references are in most cases managed by Registry Services or Human Resources. In the case of personal reference requests that staff may receive from time to time it is important to ensure that the request has come from a genuine requestor and if there is any doubt then the subject of the reference should be contacted to ensure they have given their consent.

Requests from other sources, including solicitors, fraud officers, HMRC, requesting confirmation of an individual's involvement with the University and other information should be directed to the Information Governance Officer.

In instances where the third party seeking information suspects an individual has falsely claimed to have a qualification from the University, the Academic Registrar should be consulted.

14.4.2 Requests from parents, friends or relatives

Information **may NOT be released** without explicit consent of the student.

It is acceptable to advise them that we will accept a message and, if having checked out records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at the University.

14.4.3 Requests from organisations providing financial support

The University routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g. private funders) without evidence of student consent.

14.4.4 Requests from Home Office/Immigration and Nationality Directorate/UK Visas

The University often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where we are satisfied there is a legal requirement to provide the requested information or the individual concerned has given their consent, where authorised to do so by the Academic Registrar

14.4.5 Requests from the police or law enforcement officials

The University is not legally obliged to provide information to the police, unless presented with a court order. However, the University may choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.

The University will aim to support police investigations where possible. However, the University is obliged to manage personal information in accordance with the data protection legislation.

All such requests **MUST** be referred to the Information Governance Officer.

14.4.6 Disclosures required by law

There are circumstances where the University is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order (see table above for examples of these cases).

With such requests we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

All such requests **MUST** be referred to the Information Governance Officer .

14.4.7 Information about deceased staff or students

The data protection legislation only applies to living individuals, thus a deceased staff or student's personal information is potentially disclosable under the Freedom of Information Act 2000 (FoIA). However, in doing so we must be sure that the individual whose information is sought is in fact deceased and that disclosure does not infringe the data protection rights of any third parties (e.g. parents, partners or children). There may also be an ongoing duty of confidentiality.

No information should be released unless sufficient evidence of death is provided. Such evidence may include:

- Student or staff member already recorded as deceased on records system;
- Notification of death in writing by next of kin;
- Obituary or confirmed newspaper report of death (but not if there are insufficient details to conclusively identify the student or staff member on our system); or
- Death certificate. .

Details of relatives of a deceased student or staff member should not be disclosed.

Consideration should be given to the sensitivities of the deceased individual's family where a request for disclosure is sought in the immediate aftermath of a death (e.g. by the media). Advice should be sought from senior management or the Data Protection Officer.

All such requests should be referred to the Information Governance Officer.

15. Data Sharing with Third Parties

15.1 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.

15.2 Staff who receive requests for personal information from third parties such as relatives, police, local councils etc should consult Section 14 of this Policy.

15.3 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). If no other conditions are met, then consent must be obtained from the individuals concerned and appropriate privacy notices provided.

- The University is satisfied that the third party will meet all the requirements of UK 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 UK GDPR requirements are being met

15.4 Staff should consult the Information Governance Officer if they are entering into a new contract that involves the sharing or processing of personal data.

16 International transfers of Personal Data Outside the UK

16.1 Personal data can only be transferred out of the UK under certain circumstances. The UK GDPR lists the factors that should be considered. These include whether the country to which the data is being transferred is deemed to provide an adequate level of protection to the data subjects' rights and freedoms and, if this is not the case, whether there are other appropriate safeguards in place. The transfer of personal data out of the UK will also be permitted where the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks or the transfer is necessary for one of the other reasons set out in the UK GDPR.

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

16.3 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.

16.4 Staff involved in transferring personal data to other countries should consult Information Governance Officer.

17. Data Protection Impact Assessments and Data Protection by Design

17.1 Under the UK 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.

17.2 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 UK 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.

17.3 For some projects the UK 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 on the website.

18. Research

18.1 Personal data collected for the purposes of research is covered by the UK GDPR. It is important that staff collecting such data for the purpose of research or consultancy incorporate an appropriate form of consent on any data collection form. There are some circumstances in which consent is not needed, provided certain safeguards are implemented.

18.2 Further information and guidance on data protection and research available from the Research Office.

19 Direct Marketing

19.1 Following the UK's withdrawal from the EU, the UK continues to be bound by the Privacy and Electronic Communication (EC Directive) Regulations 2003 ("PECR") which covers direct marketing via telephone, text and email.

19.2 Direct marketing is the communication to a particular individual of any advertising or marketing material. It is not confined to the advertising or marketing of commercial products or services and includes messages trying to sell goods or services and those promoting an organisation or its values or beliefs. Information promoting University events or learning opportunities at the University could constitute direct marketing and therefore it is important that the University is aware of these definitions and regulations particularly when sending out mass communications. This covers all forms of communications including by post, telephone, email and other forms of electronic messages.

19.3 It is sometimes difficult to tell the difference between a marketing email and a 'service' email. A service email is a communication that is sent to an individual that facilitates or completes a transaction, whether that is for the sale of goods or services. When trying to identify a service email the following questions should be asked:

- Are we under a legal obligation to send the email?
- Is the email part of the performance of a contract?
- Would the individual be at a disadvantage if they did not receive the email?

If the answer to any of these questions is 'yes' then the email is likely to be more of a services email than a marketing email. For instance; an email to a student about an offer on a course, paying fees or how to register would all be examples of service emails.

Marketing emails are those that promote the aims and objectives of the University such as sale of goods, services or organisational ideals. Examples would be details of how to join the sports centre which is not essential information for a student to study at the University.

19.4 Any personal details collected and held for direct marketing purposes must comply with the data protection principles e.g. it is fair and lawful, the information is only used for the purpose

it is collected for, the information is kept up to date, it is not kept for longer than necessary and is held securely.

19.5 There are some minor exceptions but in order to comply with the UK GDPR and PECR requirements governing direct marketing it is safest to assume that consent is required. Consent should normally be obtained when contact details are collected and an appropriate privacy notice provided. The consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have opted in. All subsequent marketing communications that are sent should also contain an option to opt-out with details of how the individual can request not to receive any further messages. If the University receives an opt-out request it must comply as soon as possible, there are no exceptions to this.

When requesting consent it is good practice to request consent separately for different forms of communication i.e. whether individuals agree to be contacted via post, telephone or email. This is because the different forms of communication are covered by different legislation.

19.6 Where direct marketing is communicated by telephone, staff must identify themselves and if requested, provide an address or telephone number on which they can be reached. Where cold-calling for fundraising takes place, details should first be checked against the Telephone Preference Service (TPS). Those receiving calls should be made aware of their rights to object to the calls.

19.7 There is a small exception to the general opt-in consent rule that is the 'soft opt-in' exception. This is where personal data has been collected in the context of an existing relationship with an individual and the University limits marketing to providing information on similar services/goods. In this case, the soft opt-in allows organisations to market to these individuals via electronic means without having opt-in consent. However, this can only be relied on if the individual was informed at the point of data collection that the information would be used for marketing purposes and they are given the opportunity to opt-out at that stage and in each subsequent piece of communication.

20. Impact of Non-Compliance

20.1 All staff and anyone else who processes personal data on behalf of the University are required to comply with this Policy, its supporting policies and guidance and the requirements specified in the UK GDPR. Anyone who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary or other appropriate 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.

21. University key contacts

21.1 The Data Protection Officer is responsible for:

- advising the University and its staff of its obligations under the data protection legislation;
- monitoring compliance with the data protection legislation and monitoring training and audit activities relate to compliance; and
- acting as the contact point for the Information Commissioner's Office.

21.2 The University's named Data Protection Officer is Helen Johnstone, Head of Governance and Regulatory Affairs.

21.3 In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the Information Governance Officer, Gemma Harris: infoassurance@worc.ac.uk.

22. Other relevant documentation

Personal Data Breach Incident Management Procedure

Information Security Policy

IT Regulations

Version number	Version 2.0
Author/originator of revisions	Information Governance Officer
Review Date	August 2024
Approved by	UEB – 18th August 2021
Issue date	19th August 2021
Person responsible for the document	University Secretary
Accessibility Checked	2nd August 2021