



Privacy Notice for Students

This privacy notice applies to current students and applicants who have accepted offers from the University of Worcester

What is the purpose of this document?

The University of Worcester (“we”, “our” or “us”) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your study with us, in accordance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act, together the data protection legislation.

It applies to all current students and applicants who have accepted offers from the University of Worcester. It is important that you read this notice.

The University is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under the data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current students and applicants who have accepted offers from the University of Worcester (“you” or “your”). This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

The University has also published separate notices, which are applicable to other groups and activities. Those notices may also apply to you, depending on your circumstances, and it is important that you read this privacy notice together with other applicable privacy notices:

1. [Employees, Workers and Contractors Privacy Notice](#)
2. [Visitors to the University Privacy Notice](#)
3. [Website and cookies Privacy Notice](#) (including how we monitor use of our website)
4. [CCTV webpage](#) (including information about how we use CCTV)
5. [IT Regulations](#) (which includes information about monitoring of network accounts – section 8)

This notice explains what personal data the University holds about you, how we share it, how long we keep it and what your legal rights are in relation to it.

Contact Details

We are the University of Worcester, Henwick Grove, Worcester, WR2 6A

If you need to contact us about your data: for your general student record please contact: Registry Services (studentrecords@worc.ac.uk). For other data collections please contact, in the first instance, Information Assurance (infoassurance@worc.ac.uk).

The University has a Data Protection Officer, whose contact details are: Helen Johnstone, Head of Information Assurance (h.johnstone@worc.ac.uk)

Data protection principles

We will comply with the data protection legislation. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information relating to you as a living individual from which you can be identified. It does not include data where the identity has been removed (anonymous data)

There are "Special Categories" of more sensitive personal data which require a higher level of protection.

Data that you provide to us and the possible consequences of you not providing it

The provision of most data that you provide to us is a contractual requirement. If you do not provide us with information that you are contractually obliged to provide, the consequences will depend on the particular circumstances. In some cases we may not be able to provide

you with certain services; in other cases, this could result in disciplinary action or the termination of your contract.

Other sources of your data

Apart from the data that you provide to us, we may also process data about you from a range of sources. These include:

- Data that we and our staff generate about you, such as during tutorials and in connection with your attendance and accommodation at the University;
- Your school or previous educational establishments or employers if they provide references to us;
- Fellow students, family members, friends, visitors to the University and other contacts who may provide us with information about you if and when they contact us, or vice versa.
- Data provided to us by organisations sponsoring you or providing you with financial support

The lawful basis on which we process your data

The law requires that we provide you with information about the lawful basis on which we process your personal data, and for what purposes.

Most commonly, we will process your data on the following lawful grounds:

- Where it is necessary to perform the contract we have entered into with you;
- Where it is necessary for the performance of a task in the public interest;
- Where it is necessary to comply with a legal obligation;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your data, typically in an emergency, where this is necessary to protect your vital interests, or someone else's vital interests. In a small number of cases where other lawful bases do not apply, we will process your data on the basis of your consent.

How we apply further protection in the case of "Special Categories" of personal data

"Special Categories" of particularly sensitive personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.

The Special Categories of personal data consist of data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership.

They also consist of the processing of:

- genetic data;
- biometric data for the purpose of uniquely identifying someone;
- data concerning health;

- data concerning someone's sex life or sexual orientation.

We may process Special Categories of personal data in the following circumstances:

- With your explicit written consent; or
- Where it is necessary in the substantial public interest, in particular:
 - necessary for the purposes of the prevention or detection of an unlawful act and must be carried out without your consent so as not to prejudice those purposes; or
 - for equal opportunities monitoring;
- Where it is necessary for archiving purposes in the public interest, or for scientific or historical research purposes, or statistical purposes, subject to further safeguards for your fundamental rights and interests specified in law.

Less commonly, we may process this type of data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the data public.

Criminal convictions and allegations of criminal activity

Further legal controls apply to data relating to criminal convictions and allegations of criminal activity. We may process such data on the same grounds as those identified for "Special Categories" referred to above.

Details of our processing activities, including our lawful basis for processing

We have prepared a [Record of Processing Activity](#) setting out the processing activities that we undertake, the source of the data, the reasons why we process it, how long we keep it and the lawful basis we rely on.

The table includes detailed information about how and why we process various categories of data, and the related lawful basis including (but not limited to):

- Details of which course you are studying;
- Other data that is necessary to the operation of the University/student contract or to the functioning of the University including:
 - any data about you contained in your assessed work, our assessments of your work and details of any qualifications you are awarded;
 - details of any disciplinary complaints or decisions about you;
 - your contact and accommodation details;
 - any communications you have with us, and any communications we generate about you, for example if you ask us to defer your studies to a later academic year;
 - details of any payments that you make to us, including your bank/payment card details.
- Data you and others sent us when you applied to us (including information sent to us via UCAS and your predicted grades). This includes your academic record and personal statement which we use to assess your application;
- Details of any relevant criminal convictions, allegations or charges that we ask you to declare to us either when you apply to us, or whilst you are a student, or which are reported to us, and of any Disclosure and Barring Service checks that we request.

Relevant criminal convictions or charges are those that indicate an applicant or student might pose an unacceptable risk to other students or staff.

More information is [available here](#)

- Information that you voluntarily provide to us about any disabilities or health conditions you have, and about your age, ethnicity, gender, religion and belief, and/or sexual orientation. You may also provide this information to us as part of the equality monitoring that we undertake pursuant to our legal obligations under the Equality Act 2010;
- Where you inform us of a health condition or disability, we will take this information into account when considering whether to make a reasonable adjustment under equality law and in other cases where we are legally required to;
- Data about you that we have to collect by law (for example where UK immigration law requires us to record information about you, or to report it to the immigration authorities);
- Data that we voluntarily provide about you, either whilst you are a student or after you graduate, for example if you ask us for a reference; and
- Bank and other payment details, where we need to reimburse you, or where you provide such details to us when making a payment.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

How we share your data

We do not, and will not, sell your data to third parties.

We may have to share your data with third parties, including third-party service providers and partner organisations (as detailed below)

We require third parties to respect the security of your data and to treat it in accordance with the law.

Why might we share your personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the contract with you or where we have another legal requirement or legitimate interest in doing so.

This includes for example:

- where we are required to report information about students that are subject to visa controls to UK Visas and Immigration;
- where we are required to report information to enable the University to fulfil its obligations to report information to the Higher Education Statistics Agency or its successor body in order to comply with regulatory obligations; and/or
- where we decide to report alleged criminal misconduct to the police.

It also includes disclosures where the third party is an agent or service provider appointed by the University to enable us to operate effectively, we only do this where we are satisfied that appropriate safeguards are in place to ensure adequate levels of security for your data.

More information on the categories of recipients of your data is set out in the [Record of Processing](#).

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within [the University Group](#).

Examples of bodies to whom we are required by law to disclose certain data include, but are not limited to:

Organisation	Why?
Home Office; UK Visas and Immigration	To fulfil the University's obligations as a visa sponsor
Disclosure and Barring Service (DBS)	Required for certain roles to assess an individual's suitability for positions of trust or where the role works with vulnerable people or children.
The Higher Education Funding Council for England (HEFCE)	Data submitted for the Research Excellence Framework (REF) which is a system for assessing the quality of research in higher education.
HM Revenues & Customs (HMRC)	Real time information released to HM Revenue & Customs (HMRC) in order to collect Income Tax and National Insurance contributions (NICs) from employees.

Examples of bodies to whom we may voluntarily disclose data, in appropriate circumstances, include but are not limited to:

Organisation	Why?
Other legal entities the "University Group"	We will share your personal information with other entities in the University Group as part of our regular reporting activities on company performance, in the context of a business reorganisation or the University Group restructuring exercise, for system maintenance support and hosting of data.
Agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders, or collection of a tax or duty.	For the prevention, detection or investigation of crime, for the location and/or apprehension of offenders, for the protection of the public, and/or to support national interest.
The University's Alumni Association	We will share your information in order to facilitate your membership. The Alumni Association will ask you if you wish to become a member.

Organisation	Why?
Students' Union	Your data will be shared with the Students' Union upon your registration. However, if you do not wish to join the Union you will be able to opt out at registration and at any future date.
Turnitin or other plagiarism detection software	In order to establish whether any work has been plagiarised.
Higher Education Statistics Agency (HESA)	Some information, usually in pseudonymised form, will be sent to the HESA for statistical analysis and to allow government agencies to carry out their statutory functions.
Occupational Health providers	For some courses it is necessary for students to have an occupational health assessment. Students will be asked to provide their data to the Occupational Health provider who will provide an assessment to the University.
Third party service providers	To facilities activities of the University including activities that are carried out by third-party service providers and partner organisations. Any transfer will be subject to an appropriate, formal agreement between the University and the third party service provider.

Where information is shared with third parties, we will seek to share the minimum amount of information necessary to fulfil the purpose.

How secure is my information with third-party service providers and other entities in the [University Group](#)?

All our third-party service providers and other entities in the [University Group](#) are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes (as written in the contract between us) and in accordance with our instructions.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business requirement to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details

of these measures may be obtained from the Data Protection Officer [Helen Johnstone, Head of Information Assurance email: infoassurance@worc.ac.uk]

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Sharing your data outside the European Union

The law provides various further safeguards where data is transferred outside of the EU.

When you are resident outside the EU in a country where there is no “adequacy decision” (a country outside the EU that ensures adequate level of data protection due to its domestic laws or international commitments) by the European Commission, and an alternative safeguard is not available, we may still transfer data to you which is necessary for performance of your contract with us, or to take pre-contractual measures at your request.

We intend to transfer the following information about you to the following countries:

<u>Country</u>	<u>Recipient</u>	<u>Reason for transfer</u>
USA	To allow access to certain IT provision	Staff name and email address
USA	In relation to vehicle hire	Staff name and contact details when vehicle hire is arranged.

In the case of the USA the providers used by the University are part of the EU Privacy Shield Framework which means the Commission has decided that it has an adequate level of protection for personal data for the time being.

Data Retention

How long we keep your data

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our [Records and Document Retention Schedule](#)

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Retention periods may increase as a result of legislative changes, e.g. an increase in limitation periods for legal claims would mean that the University is required to retain certain categories of personal data for longer. Any such changes will be reflected in updated versions of our Records and Document Retention Schedule which is reviewed on a three year basis.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. We may keep anonymised statistical data indefinitely.

Once you are no longer a student or alumni of the University we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your study with us and until after you have graduated or otherwise completed your studies with us.

Your rights in connection with personal information

Where we are processing your personal information on the basis of your consent, you always have the right to withdraw that consent.

Under certain circumstances, by law you have the right to:

- **Request access to your personal information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction of the personal information that we hold about you.** This enables you to ask us to correct any incomplete or inaccurate information we hold about you.
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing of your personal information** where we are processing your information on the basis of our legitimate interest (or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes. The lawful basis for any particular processing activity we carry out is set out in our detailed table of processing activities.
- **Request the restriction of processing of your personal information.** This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Suspend processing of your personal information,** for example if you want us to establish the accuracy of the data we are processing.
- **Object to any direct marketing** (for example, email marketing or phone calls) by us, and to require us to stop such marketing.

- **Object to any automated decision-making** about you which produces legal effects or otherwise significantly affects you.
- **Request the transfer of your personal information to another party.**

Please be aware that these rights are subject to certain conditions and exceptions as set out in the data protection legislation.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer [Helen Johnstone, Head of Information Assurance email: infoassurance@worc.ac.uk] in writing and they will explain any conditions that may apply.

Further guidance on your rights is available from the Information Commissioner's Office (<https://ico.org.uk/>). You may also wish to contact the University's Data Protection Officer [Helen Johnstone, Head of Information Assurance email: inforassurance@worc.ac.uk] if you are considering how or whether to exercise your rights.

You have the right to complain to the UK's supervisory office for data protection, the Information Commissioner's Office if you believe that your data has been processed unlawfully.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Information Assurance (infoassurance@worc.ac.uk). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Further guidance on your rights is available from the Information Commissioner's Office (<https://ico.org.uk/>). You have the right to complain to the UK's supervisory office for data protection, the Information Commissioner's Office at <https://ico.org.uk/concerns/> if you believe that your data has been processed unlawfully.

Future changes to this privacy notice

We may need to update this notice from time to time, for example if the law or regulatory requirements change, if technology changes, if the University makes changes to its procedures, or to make the University's operations and procedures more efficient. If the change is material, we will give you not less than two months' notice of the change so that you can decide whether to exercise your rights, if appropriate, before the change comes into effect. We will notify you of the change by email.

Version number	Version 1.0
Author/originator	Head of Information Assurance
Review Date	1 st May 2019
Ratified/authorised by	VCAG
Issue date	TBC
Postholder/s responsible for review	Head of Information Assurance