



University of
St Andrews

University privacy notice: student recruitment

Document type	Policy
Scope (applies to)	All students
Applicability date	15/04/2020
Review / Expiry date	15/04/2021
Approved date	07/07/2020
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Information governance and management/Data protection
Purpose	To advice people how their personal data are used by the University

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	First version	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	16/04/2020

1. Purpose

The use of information that relates to people i.e. personal data, which is collected or received and then used by the University is legislated governed by the European and UK data protection laws, specifically:

- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“the GDPR”); and*
- *The Data Protection Act 2018 (“the DPA”).*

These data protection laws set out via a series of principles how organisations are expected to manage and safeguard personal data. In addition, the legislation provides a number of rights to individuals, so that they have a degree of control over their personal data, with access to rights of redress, if it is found that their personal data has not been managed correctly. The University takes these obligations seriously.

One of the principles of data protection legislation is transparency, with one of the data protection rights being the right to be informed. This means that organisations that collect/receive personal data must clearly and fully inform the individuals concerned, in writing, normally when personal data is collected, how their personal data will be used. Organisations are expected to provide those details through a privacy notice.

A privacy notice should:

- confirm the identity of the organisation, that is responsible for making use of personal data in line with the data protection legislation, along with providing the contact details of who to approach with questions on how such data is managed;
- set out how personal data will be used and the legal basis underpinning that use;
- identify other organisations and/or individuals that personal data may be shared with (recipients);
- note when personal data may be transferred to a country outwith the European Economic Area (“the EEA”) and what protections will be put in place to safeguard those data;
- state how long personal data will be retained, or, where that is not possible, the criteria used to determine this;
- summarise the rights available to individuals under data protection legislation and explain how those rights can be exercised;
- advise on the right of complaint to the data protection regulator i.e. the UK Information Commissioners Office (“the ICO”);
- note where there are any statutory or contractual obligations to provide an organisation with personal data; and
- confirm where automatic decision-making takes place, including the provision of details of profiling and any consequences of such uses.

The purpose of this privacy notice is to inform individuals how their personal data will be used by the University and relevant third parties; the legal basis which underpins the use of personal data by the University or the transfer of personal data to others; what rights are available to individuals and how those rights can be exercised; and who to contact should there be any questions or issues of concern on how personal data are being used.

The statement aims to set a reasonable expectation amongst individuals as to how the University will use and manage their personal data during their time at inquiry, application, and whilst at the University and following their departure.

2. The identity and the contact details of the controller

University of St Andrews, College Gate, North Street, St Andrews, KY16 9AJ, Fife, Scotland, UK.
The University is a charity registered in Scotland, No SC013532.

3. The contact details of the University Data Protection Officer

Mr Christopher Milne, Head of Information Assurance and Governance, University of St Andrews,
Email dataprot@st-andrews.ac.uk

4. The purposes for which the University will make use of inquirer and applicant personal data

Individuals often engage with the University before they decide whether to apply to the University; this can be through a series of events such as visiting/open days, or earlier through participation events run via schools. Personal data from inquirers is used predominately as: a point of contact, to manage any questions individuals may have, to organise invitation and attendance at recruitment events, to understand their interests so that we can tailor events/activities that match.

The personal data of applicants is used by the University to: administer and consider an application; to maintain contact e.g. to provide updates on an application and to answer any questions that applicants may have; to advise applicants and/or family/nominated contact(s) about the University and services that may of relevance e.g. University managed student accommodation and to confirm decisions made on applications. The University Admissions Policy also sets out how personal data are used to manage applications.

The University may also use personal data of inquirers/applicants for the following purposes

Communication

- The University may also send additional communications covering areas believed to be of interest and importance to applicants when considering whether to study at the University. This is to fulfil our pre-contractual obligation of informing applicants of all relevant information pertaining to study and student life at St Andrews throughout the application process until such times as a person registers. Applicants can opt out of these additional communications at any time.

Alternative offer

- Where it has not been possible to make an offer, the University may review and re-consider an application to suggest or make an alternative offer, where it is in an applicant's and the University's legitimate interests to do so.

Applicant and Student record administration

- The activities involved in creating an applicant record, which records your application and key communications between applicants and the University. Where a place is offered details from the applicant record will form the basis of a student record.

Tuition fee administration

- The activities involved in determining tuition fee classification levels.

Financial support

- The admission and provision of financial support (grants, loans and bursaries etc.) This may include liaison with sponsors.

Verifying applications

- Where University staff responsible for admissions decisions suspect that an academic document may not be genuine, the University will check the authenticity of the academic

document with either the awarding body or the UK National Academic Recognition Information Centre (UK NARIC). In such cases, and in order to verify authenticity only a copy of the relevant document will be shared.

Eligibility to study in the UK

- If a Tier 4 student visa is required to study in the UK, then personal data will be shared with UK Visas and Immigration (UKVI) in order to create a Confirmation of Acceptance for Studies (CAS).

Providing support services

- Providing and administering access to services and facilities provided by or through the University as necessary to support teaching, learning and, and time spent with the University. This will include understanding if reasonable adjustments that are requested to support a disability can be made.
- Where an offer of a place is made and accepted, personal details will be used to set up and provide access to services – those may include:
 - A University email address and access to central file storage on the University network and printing services;
 - University Library e.g. lending, access to on-line materials;
 - Careers guidance;
 - Production of a University student identity card, which provides access to buildings and other facilities such as printing; and
 - The admission and provision of health care services provided by or through the University.

Equality and diversity

- Monitoring and reporting on equal opportunities within the University.
 - This will involve the collection of data on a range of activities and the participation/engagement with those e.g. student recruitment and admission; analysing data in relation to equality for people by gender and/or protected characteristics, as defined by legislation; preparing and submitting formal reports of equal opportunities monitoring internally and to external organisations. Providing information on protected characteristics is entirely optional; if a person chooses not to provide such information there will be no detriment.

Imagery (still photographs and video)

- The University may from time-to-time take photographs and/or video imagery of events or activities across the institution. When such activities take place, notice will be available at the location; if individuals do not wish to feature, they can (a) avoid that area or (b) make themselves known to the photographer(s) who will be identifiable. The photographs and imagery taken will be used to promote the University and life at the institution in University and/or third-party publications. Photographs and imagery may also then feature as part of the University archive.

Public Safety – including the University community

- Images captured by Close Circuit Television (CCTV) systems operated by or on behalf of the University will be used for purposes of providing a safe campus environment and for the prevention and detection of crime, and in investigations where it is believed that University policy and/or regulation may have been breached.

Management reporting and forecasting

- The University may use personal data of inquirers/applicants when producing/compiling management reports, which may involve statistical data analysis; and the dissemination of those reports for the purposes of planning, forecasting and decision making. Data will be aggregated and will not focus on individuals.

- When producing/compiling statistical data sets and management reports, a range of safeguards such as pseudonymisation will be put in place, as appropriate, to protect privacy.

Sector and Statutory Reporting

- The University may produce statistical and other reports for agencies/authorities to whom the University has an obligation to report, such as funding bodies, the Higher Education Statistics Agency, the Scottish Government.

Complaint handling

- Where complaints are made that the University has not followed its Admissions Policy when managing an application, personal data will be used when assessing and/or investigating a complaint.

5. Legal bases for processing personal data

The University maintains a catalogue of the purposes of processing personal data and the corresponding legal basis. For full details please see www.st-andrews.ac.uk/Data-Protection, or email dataprot@s-andrews.ac.uk.

The most common legal basis that the University will rely upon for the lawful processing of student personal data for the purposes/activities introduced, above, are outlined below.

- **Contract or preparation for entry into a contract**

- In this context, the contract that exists between a student and the University, when an individual accepts an unconditional offer of study i.e. –
 - The majority of the personal data that the University collects (or creates) from both prospective and current students is used by it so that it can provide access to a range of educational services and facilities that are consistent with supporting the contract relationship. For example, when applying for a place at the University, many prospective students provide the University with a passport style photograph. The University will use that information to produce a Student ID card for that individual, so that it is ready for collection during arrivals weekend or matriculation. Following matriculation, the University could also make use of student photographs by circulating these to lecturers so that they can begin to recognise students that they will work with. The use of the photograph in that instance is consistent with the University meeting its contractual obligations (administering and providing for a high quality student experience).

- **For compliance with a legal obligation to which the University is subject.**

- In prescribed circumstances the University is required by law to make available to other agencies and authorities personal information concerning employees. Examples include statutory returns to the Scottish Funding Council, making returns to Local Authorities for purposes of maintaining an electoral register and retaining evidence of proof of entitlement to study in the UK, for the Home Office.

6. How the University collects your personal data?

Personal data from inquirers is collected from individuals when they engage with the University. Details from some applicants are provided via the Universities and Colleges Admissions Service, where applications are made via UCAS, or from individuals or their agent when a direct application is made to the University. In some instances details are received from Partner Institutions.

For applicants who have an educational background from the UK, the University may also consider 'contextual data' that is socio/economic data of relevance to a place of study or an area where an applicant may have come from. Those details are used to inform the decision making process,

notably where the University has a commitment or requirement to promoting equality of opportunity. The University Admissions Policy and supporting statement on the collection and use of Contextual data provides additional details.

7. The recipients or categories of recipients of the personal data, if any

Within the University

Personal data will be shared within the University as appropriate with individuals who are directly involved in student admissions (including inquiries) and recruitment, and for successful applicants, Professional Services such as the University Library and IT Services.

Outwith the University

The University may disclose certain personal data to external bodies as categorised below. At all times, the amount of information disclosed and the manner in which it is disclosed will be in accordance with the provisions and obligations of UK and European data protection legislation. Please note this is not an exhaustive list.

Disclosure to for the purposes of	Details
Academic sponsors	The University will pass a limited amount of information to sponsors for the purpose of managing invoices and the payment of fees. The University will not pass information to a sponsor concerning academic performance and/or progression unless this is a condition of sponsorship with which a student has accepted or without first having secured consent of the individual concerned.
Agents/suppliers of the University	<p>The University will pass onto named agents/suppliers personal data as necessary to enable them to provide services to the institution under contract. This may also include sub-contractors, engaged by agents/suppliers. This includes outsourced ICT services, such as email.</p> <p>Before an agent/supplier of the University, or a sub-contractor(s) engaged by an agent/supplier, will be given access to personal data for which the University is responsible as data controller, contractual terms will exist between the University and that party which:</p> <ul style="list-style-type: none"> ○ specify and limit the uses that can be made of the personal data it is provided with or given access to through the University; and ○ establishes to the University's satisfaction that the agent has in place sufficient organisational and technical means to protect personal information made available to them against accidental loss or any form of unauthorised access and subsequent use.
Higher Education Statistics Agency ("HESA")	The University transfers personal data to HESA for statistical analysis and to enable the Scottish Government and/or relevant agencies e.g. The Scottish Funding Council ("the SFC") to undertake statutory reporting duties. HESA data collection notices which specify how that body may use your personal data are available from: https://www.hesa.ac.uk/about/regulation/data-protection/notices Accessed 06 April 2020.
Home Office: UK Visa and Immigration	To provide evidence that a person is entitled to study and remain in the UK.
Next of Kin	The University will pass onto next of kin, where those details have been provided to the institution, such information as necessary should an emergency arise e.g. a person has suffered from an accident and has been taken to hospital for treatment.
Partner institutions	The University will share personal data of students who have opted to undertake their study with a partner institution as necessary to manage and administer that individual's education with the University and that body.
References	Where a referees contact details have been provided the University may contact them with limited information about you to request they submit a reference. Where references have been provided, the University may contact the referee to clarify information. The University may also ask a referee to verify information you have provided to us where relevant.
Relatives, guardians or carers of inquirers/applicants	Under normal circumstances the University will not disclose any personal data of an inquirer/applicant to any of their relatives, guardians, or carers etc. without consent. Individuals can inform the University if we can talk to a third party about an application on their behalf.

The Student Loans Company ("the SLC")	Information will be shared with the SLC to administer applications for loans and other forms of financial assistance administered by SLC, which individuals have applied for.
---------------------------------------	---

Details of transfers of personal data to countries outwith the EEA

Where an applicant is domiciled overseas then personal data may be transferred to you and/or an Agent, as necessary to manage an application.

The period for which personal data will be stored, or if that is not possible, the criteria used to determine that period

For successful applicants, information about an application will be retained during your time as a student and for a period of six years afterwards, after which elements of your personal data will be destroyed. Details of unsuccessful applicants will be retained by the University and destroyed two years after the end of the application cycle. There may be occasions when the University is required to keep personal data for longer time periods. Where this is the case, this will be documented in the University Records Retention Schedule. Best practice records retention periods, notably those published by the Joint Information Systems Committee ("the JISC") will be used to help determine the relevant storage times. Details of JISC recommended retention periods are available from: <http://bcs.jiscinfonet.ac.uk/he/default.asp>.

Rights available to individuals

European and UK data protection legislation provides individuals with a number of rights regarding the management of their personal data, these rights are:

- The right of access to your personal data, commonly referred to as a subject access request, which involves the following being carried out within a calendar month:
 - Confirmation that personal data is being processed.
 - Access being given to your personal data (provision of a copy), unless an exemption(s) applies; and
 - The provision of supplementary information e.g. an explanation of how your personal data is processed and who this is shared with.
- The right to rectification, which may involve:
 - The University working to correct any inaccuracies in personal data or to address any omissions, which may require personal data to be annotated to acknowledge that this is incomplete.
- The right to erasure (the deletion of personal data, in specific circumstances), which is commonly referred to as the right to be forgotten, which may involve:
 - The University destroying specific personal data.
- The right to restrict processing, which may involve:
 - The University agreeing to stop making use of specified personal data e.g. where those data are contested, in terms of accuracy.
- The right to data portability, which may involve:
 - The University providing you with a copy of elements of your personal data that exist in machine readable form that you have given to the University.
- The right to object. Individuals have the right to object to, the University making use of personal data where:
 - Either legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) is the legal basis that the University has relied on for making use of the said data;
 - The data in question is used for direct marketing (including profiling) – in such circumstances the use of personal data must stop when an objection is received; and
 - The data in question is used for the purposes of scientific/historical research and statistics.
- Further details on the right to object are available from the University website.

In many instances, the rights introduced above are qualified i.e. in certain circumstances they are limited or they may not be available, and these may be further constrained by UK legislation, e.g. where personal data is only used for research or statistical purposes. Details of note include:

- The right of subject access can be refused or an administrative fee charged, where a request is found to be manifestly unreasonable or excessive. In addition, where a request is found to be complex or numerous requests are made, then the University can extend the time for compliance by 2 months.
- The right of erasure does not provide an absolute right to be forgotten. This right is only available in limited circumstances – notably where the legal basis for processing personal data is for the performance of a contract or linked to a statutory requirement, then the said right is not available. The University does not have to comply with a request for erasure where personal data is processed for the following reasons:
 - to exercise the right of freedom of expression and information;
 - to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
 - In many instances the University processes personal data for the performance of its public tasks e.g. teaching, learning and research.
 - for public health purposes in the public interest;
 - archiving purposes in the public interest, scientific research historical research or statistical purposes; or
 - the exercise or defence of legal claims.
- The data portability right is only available to personal data which an individual has directly provided to the University and where the legal basis for processing that data is either contract or consent, and where the said personal data are processed by automatic means.

These rights have to be met by the University and any other organisation that takes decisions about how or why your personal data is used. Details on how to access those rights are available from the University website, or you can contact dataprot@st-andrews.ac.uk.

8. The right to lodge a complaint with a supervisory authority

If you believe that the University has not made use of your personal data, in line with the requirements of the law, you have the right to raise this with the regulator i.e. the UK Information Commissioner Office's ("the ICO").

Details on how to contact the ICO are available online, at:

- <https://ico.org.uk/global/contact-us/>

9. Whether there is a statutory or contractual requirement to provide personal data and the consequence where no personal data are provided

In the context of applying for a place at the University or studying, circumstances can arise where an individual has an obligation either under law, or via their contract with the University to provide certain information. Failure to provide information in those circumstances may have consequences e.g. if correct bank details are not provided, then the University is unlikely to be able to make any bursary payments that are due until such time as an error is corrected. If a person fails to disclose a criminal conviction, which may have an impact on their place at the University, then action under disciplinary policy may arise, which could lead to termination of studies.

- Inability to provide proof of the entitlement to study in the UK, may impact negatively on the University ability to maintain a place of study.

10. The existence of automated decision-making including profiling

The University does not make use of profiling or automated decision-making processes. Some processes are semi-automated but a human decision maker will always be involved before any decision is reached in relation to you.

11. Revision of the Privacy Notice

This Privacy Notice will be reviewed at regular intervals. The review period will be approved by the University and recorded on the accompanying coversheet. Any significant change to relevant legislation, the University Admissions policy may trigger an earlier review.

12. Availability

This Privacy Notice will be published on the University website.

Should a copy of this Privacy Notice be required in another form, including orally i.e. an audio recording, please contact dataprot@st-andrews.ac.uk.