University privacy notice: Post graduate research students

Author	Head of Information Assurance and Governance
Approved by	University Information Compliance Group
Approval date(s)	24 April 2018
Review date	May 2019
Version	1.0
Document type	Privacy notice
Activity/Task	Information governance and security
Keywords	GDPR, DPA 2018
Confidentiality	PUBLIC

Version Control Table

Version Number	Purpose / Changes	Author	Date
1.0	First version	C Milne	24 April 2018

Contents

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 through 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 re-dress, 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 postgraduate research students ("PGR students") as to: how their personal data will be used by the University and relevant

third parties in the context of their time at the University and when their time at the University has come to an end; 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 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, Buts Wynd, North Street, St Andrews, KY16 9AJ, Fife. Email dataprot@st-andrews.ac.uk

4 The purposes for which the University will make use of students' personal data

The University may make use of a PGR student's personal data both during and after their time at the University for a variety of reasons in connection with the following processes and activities. The University maintains a catalogue of the purposes of processing personal data and the corresponding legal basis. For full details of all of the purposes of processing and the associated legal basis, please see the University's legal basis for the processing of personal data, www.st-andrews.ac.uk/Data-Protection, or email dataprot@s-andrews.ac.uk.

4.1 Academic administration

4.1.1 PGR Student admission

- The administering of applications to read for a postgraduate research degree at the University.

4.1.2 PGR Student registration

- The range of activities involved in registering PGR students in an academic programme, including:
  - Confirming payment of fees, including validating evidence of awards and managing the transfer between Master of Philosophy and Doctor of Philosophy degree programmes as necessary.

4.2 PGR Student record administration

- The activities involved in creating a student record and thereafter compiling and maintaining accurate records of progress, including the recording of research outputs which may include publication within institutional repositories, websites etc.; attainment; conduct and making PGR students'

records, and aggregated PGR student data and analyses available throughout the University as appropriate to support other institutional activities.

4.3 PGR programme co-ordination

- The activities involved in co-ordinating the delivery of PGR programmes, including:
  - Scheduling and administering research supervision; organising fieldwork; scheduling the submission, marking and return of assessed work, and monitoring compliance with these schedules; monitoring students' attendance.

4.4 PGR annual reports and progress review

- The activities involved in the annual submission and review of a [PGR] Student Progress Report.
- Making decisions on academic progression, which may involve the exchange of information between Schools, Student Services and the Principal's Office.

4.5 PGR Student assessment administration

- The activities involved in administering the work of internal and external examination of PGR student academic work, including the administration and management of examination by viva-voce.
- The determination whether academic work submitted is consistent with University requirements. This may include the application of measures to detect and prevent academic dishonesty.

4.6 PGR Student academic appeals

- The activities involved in considering and managing appeals.

4.7 PGR Student discipline case handling

- The activities involved in conducting investigative and disciplinary proceedings concerning alleged/proven breaches of the institution's regulations, including those concerning misconduct e.g. academic, non-academic, research.

4.8 Academic award administration

- The activities involved in administering the conferment of the institution's academic awards via graduation, including the recording and public broadcasting of ceremonies and maintaining a record of those awards within the University archive.

4.9 Publication of research outputs

- The activities involved in adding a Postgraduate Research Degree thesis to the University Library collection and the British Library eThos repository, and making that item available; promoting research activities and outputs via the University's and related web sites and other research directories, databases and related management information systems.

4.10 Communication

4.10.1 Directly engaging with PGR students

- University student email addresses and/or other contact details provided to the University will also be used by the University and any of its agents to alert individuals to news, events and other matters relevant to the operation of the University, their studies and/or research and to the services/facilities that are available to PGR students. Communication with the student body may also include:
  - Providing PGR students with updates by email on what is happening across the University;
  - Organising the election and/or appointment of student representatives to the institution's governing body and executive committees;
  - Operating student suggestion schemes; and
  - Conducting general student surveys and consultations.

4.11 Complaint handling

4.11.1 Internal management of complaints

- Investigating and determining how responses to complaints, assessed via the University Complaints Handling Procedure, will be made.
  - E.g. review of correspondence between the University and PGR students.

4.11.2 Responding to investigations by the Ombudsman

- The development and submission of responses from the University, when responding to investigations undertaken by the Scottish Public Services Ombudsman (“the SPSO”).

4.12 Financial support

- The admission and provision of financial support (grants, loans and bursaries etc.)

4.13 Information and Communications Technology (“ICT”) Management

4.13.1 ICT systems operation management

- Logging and managing ICT fault reporting and resolution.
- Maintaining a record of ICT resources issued/made available to individuals and the provisioning of those services.

4.13.2 ICT systems development and testing

- The University may also, where required, use copies of elements of the personal data of PGR student during the development and testing of institutional IT systems/services. However, the use of personal data for systems development and/or testing will be kept to a minimum. Wherever possible personal data will first be randomised or scrambled, so that those data are constituted in such a way that they do not relate to any known person.

- Testing is undertaken within specific test environments i.e. a duplicate of a real world 'live' system/service. Actual personal data will only be used as a last resort. Testing is undertaken to help ensure that new developments or system changes will be effective, operating as planned and will not cause loss or damage to data in a live environment. Personal data which is held and maintained in live systems/services will not be affected in any way. Data will not be kept in a test environment for longer than is necessary for testing purposes, and data in that environment will not be used for any purpose other than testing. Appropriate security precautions and permissions will be applied to the data and any copy used for testing will be deleted after testing and any other reviews have been completed.

4.13.3 ICT systems security management

- Opening, closing and managing system user accounts.
  - This will include accessing file shares and email services for business continuity purposes when an individual is not available, as per published University policy and protocols.
- Creating and managing logs of system/service use.
- Monitoring use of University ICT systems and/or devices to ensure compliance with institutional policies and relevant legislation.
- Investigating the use/operation of University ICT systems and/or devices to understand whether compliance with institutional policies and relevant legislation has been made or otherwise.
- Responding to actual or suspected security breaches or incidents.
  - This may include working to understand what systems and services an individual has made use of.
- Sanitisation of ICT hardware before disposal, or following loss.
  - This may include, the University remotely destroying all data held on a device, under the University's control to contain/prevent the loss of data to a third party e.g. when a University mobile (smart) phone is stolen or lost.

4.14 Insurance claims management

- Administering the review and settlement of claims against insurance policies.
  - This will include reviewing claims and liaising with relevant parties, including insurers, claimants and legal advisors.

4.15 Legal Affairs/litigation Management

- Handling claims by or against the institution which may not proceed to litigation and/or which may result in out of court settlement.
- Managing legal actions by or against the institution.
  - Preparation of evidence such as witness statements and/or the supply of case materials to a solicitor, Court, Tribunal etc. This may include securing evidence from the student record and other records/documentation held by the University to pursue or defend a claim.

4.16 Management reporting

- The activities involved in 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.
- 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.

4.17 Media Management

- Media communications.
  - e.g. Issuing press releases on University activities and responding to media inquiries.
- Publishing details of PGR student involvement in University activities via the institution's website and other publications.

4.18 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.
- Data from the University access control systems and/or logs of network and ICT facilities usage may be used to understand or determine whether a person was in a particular location or making use of a particular resource at a point in time. Such information may be used to support investigations regarding whether University Policy has been breached or for the prevention and detection of crime, or to identify the presence of a person where there are legitimate concerns over their personal safety and wellbeing.

4.19 Research

4.19.1 Research planning and design

- Defining project roles and responsibilities; securing necessary ethical reviews and approvals (internal and external as appropriate); determining requirements for project resources; preparing research proposals.

4.19.2 Research funding administration

- The activities involved in; applying for research grants and other forms of financial support; providing progress reports to research funders on academic performance and/or research outputs.

4.20 Scholarship, fellowship and prize administration

- The activities involved in administering the award of scholarships, fellowships and prizes.

4.21 Sector and statutory reporting

- Statistical processing (compilation, monitoring and dissemination internally and externally to agencies/authorities to whom the University has an

obligation to report, such as funding bodies, the Higher Education Statistics Agency, the Scottish Government).

4.22 Support Services

- Providing and administering access to services and facilities provided by or through the University as necessary to support teaching, learning and research, and time spent with the University. This will include face-to-face and on-line services and facilities, such as:
  - A University email address and access to central file storage on the University network;
  - Those available from the 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;
  - The admission and provision of health care services provided by or through the University;
  - The administration and provision of welfare and pastoral services. This could include professional counselling services and health care services provided by or through the University; and
  - Membership of the University Athletics Union, through which PGR students can join affiliated sports clubs.

4.23 Teaching and learning

- The organisation, delivery and assessment of teaching and learning, which lead to academic awards. This will include face-to-face and on-line services and facilities such as:
  - The organisation and administration of activities to assess your educational achievement and progress, e.g. written examinations, on-line tests, viva-voce;

4.24 Tuition fee administration

- The activities involved in determining tuition fee classification levels and collecting fees as appropriate.

4.25 University Archive

- Core elements of the student record will be held in perpetuity within the University archive (both physical and electronic). Such information will be used to develop and sustain the institution's corporate memory. This will assist the University in its corporate decision making and in meeting its wider societal obligations, such as the provision of references, or developing an understanding of the composition of the student body over time.

5 The 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.

- **For the performance of a task carried out in the public interest or in the exercise of official authority vested in the University.**
    - The University has a number of powers delegated to it, through legislation, which give it the authority to conduct a number of activities, which include teaching, learning and research.
        - For example, the Universities (Scotland) Act 1889 c. 55, section 7 (1) (Powers of Senatus Academicus) i.e. "To regulate and superintend the teaching and discipline of the University [and to promote research[1]]." Where the University is required to use personal data to deliver the institution's taught programmes, it can rely on the authority from the said legislation as a legal basis to do so. An example would include maintaining details the modules a student was registered on.

- **For protecting the vital interests of individuals.**

[1] As amended by the Universities (Scotland) Act 1966, s8(1).

- Vital interests in this context mean protecting the life and wellbeing of an individual. For example, the University would inform the emergency services of known medical conditions of a student where they had lost consciousness.

6 The recipients or categories of recipients of the personal data, if any

6.1 Within the University

In order to meet its contractual obligations with PGR students and/or to perform public task e.g. teaching, learning and research etc. and to meet any legal or regulatory obligations the University will form time to time pass personal data between Schools, Service Units and the Principal's Office as necessary to manage activities concerned with the:

- provision of higher education and training;
- the promotion of research;
- provision of student support services;
- the management of the University, including the student body; and
- membership of sports clubs affiliated to the University Athletics Union.

6.2 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 and/or research 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 PGR student has accepted or without first having secured consent of the individual concerned.
Agents/suppliers of the University	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. 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: ○ 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.

British Library	The University will provide the British Library Document Supply Centre and/or other participating libraries the personal details of individuals who seek to access materials via inter library loan.
Courts of law and Tribunals	The University will provide personal data to (1) a named entity or person, when instructed to do so by Court Order or decree, unless a successful challenge to such an order is made; or (2) to a third party contractor, for example a debt collection agency, for administration and execution of such Court order or decree.
Debt collection agencies	The University may provide personal details to a debt collection agency where it is necessary to seek resolution on outstanding monies owed to the University and/or the return of resources to the University.
Disclosure Scotland	Administration of the Protecting Vulnerable Groups ("PVG") scheme i.e. criminal record checks for individuals, before they take up duties which would bring them into contact with persons in vulnerable groups.
External supervisors	The University will share details of student academic performance with external supervisors, which will include thesis drafts and submissions for the purpose of assessing the quality of academic provision.
Government agencies and local authorities, with statutory powers to obtain information from the University as a higher education institution and/or an employer.	For example, the Section 9A of the Representation of the People Act 1983, requires that the University pass on to the Electoral Registration Officer all information as necessary to maintain the register of electors.
Higher Education Institutions ("HEIs")	The University transfers information between HEIs where a PGR student is on a joint degree programme, which can include students working in a Research Council Doctoral Training Programme and/or Centre for Doctoral Training.
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/files/HESA_Staff_Collection_Notice_2017-18.pdf, Accessed 20-December-2017.
HM Revenue and Customs ("HMRC")	Transfer of personal data, as necessary for the assessment of and collection of taxes and other duties.
Home Office: UK Visa and Immigration	To provide evidence that a person is entitled to study and remain in the UK.
Law enforcement agencies	The University may provide personal data to law enforcement agencies, where there is just cause, for the: prevention and detection of crime; apprehension and prosecution of offenders; assessment or collection of any tax or duty or imposition of a similar nature; or any matters pertinent to national security. Prior to the release of personal data to the Police or a relevant authority, for the purposes noted, above, the University will first satisfy itself that a request is legitimate and that the disclosure of the personal data is lawful. In this regard, the University will make reference to the provisions from relevant data protection legislation.
Media outlets	The University may pass on personal data to the media in terms of press releases, which may provide details of a person's study and/or work at the institution e.g. participation in a research programme.
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.
Payment processing	The University will make available to third party on-line payment processors e.g. WPM Education, minimal data (i.e. student ID number and date of birth) that will enable that party to validate on-line payments made by students for goods/services purchased from the University.
Professional bodies and learned societies	Where research is undertaken in a professional setting then there may be an expectation that external standards for ethical approval and other aspects of research design and management will apply. This can include the National Health Service when research is funded and/or coordinated via that public authority. PDR student details, including progress reports may be shared with professional bodies and learned societies, so that that such bodies can undertake their constituted tasks. Should a PGR student be accused of professional misconduct, then there may be a requirement on the University to share details with professional bodies and learned societies for the purposes of investigation and any follow-up actions.
References and/or confirmation of student performance	The University may release personal information concerning a current or former student to a third party in response to a request for a reference when it has the prior consent of the individual concerned. The University routinely receives enquiries from potential employers seeking to validate claims made regarding educational performance, prior to offering employment to students or former students. The University will not release any personal data without having secured or confirmed the necessary consent from the individual concerned.
Regulators	To fulfil statutory responsibilities of the regulator e.g. when conducting investigations. Examples include the Health and Safety Executive and the Scottish Public Services Ombudsman.
Relatives, guardians or carers of students	Under normal circumstances the University will not disclose any personal data of students to any of their relatives, guardians, or carers etc. without the consent of a student. The University may, however, contact a student to inform them that another party wishes to make contact. Where a student has left the University for whatever reason, or they are not in attendance (e.g. a leave of absence) and a third party makes enquiries about them, or seeks to contact them, assuming that they can be reached at the University, the University may (as a last resort) confirm with that party that it is unable to assist the enquirer, where the University cannot contact the individual concerned. By stating that the University cannot provide any such assistance will in itself confirm that an individual is not in attendance at the University. However, the reasons for non-attendance will not be disclosed.
Research bodies/funders and publishers	Personal data will be exchanged with research bodies and funders etc. as necessary to make application for research funding and to make any reports/updates that a funder or research body requires of the University in connection to research. Publication details, and details of research outputs may be made available to support publications and citation indexes, and to support assessments of the University's research outputs e.g. the Research Excellence Framework. Personal data may be shared with publishers; both when arranging for and managing the publication of materials and in instances where allegations of research misconduct have been made, where this concerns published materials.
The Equalities Challenge Unit	To support reporting requirements allied with the Athena SWAN charter.
The public	Personal data in publicly available research profiles, including bibliographic/publication details, datasets and other research outputs and

	activities will be made available; where an embargo applies publication of research outputs/thesis will be delayed. Personal data can be released into the public domain, where it is fair and lawful to do so, in response to information requests managed under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. Personal data may also be made available to the public, via information sources, to which the general public have legitimate access e.g. elements of the University web site and publications such as prospectuses.
The University of St Andrews Students' Association ("the SA")	The University will pass onto the SA details of students so that the Association may then provide the relevant membership services to students, as per the relevant provisions of the Education Act 1994. If a student wishes to exercise their right not to be a member they can do so by contacting the SA offices.

6.3 Details of transfers of personal data to countries outwith the EEA

Where a PGR student of the University is studying overseas, undertaking fieldwork and/or attending conferences/meetings etc. then personal data may be transferred to make all arrangements, as necessary associated with travel to and from, accommodation and attendance at an event.

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

In many instances, the University will be required to keep personal data about students' for the duration of their studies and for up to six years following the end of their time with the University, after which juncture elements of the student record will either be destroyed or retained, depending on legislative and University business requirements.

There may be occasions when the University is required to keep personal data for longer time periods. Where this is the case, 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.

6.5 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.

7 Where processing is based on consent (or explicit consent), the right to withdraw consent at any time

Circumstances may arise where it will be necessary for the University to seek the consent of PGR students so that it can process personal data. However, this is likely to be a relatively rare occurrence, as the majority of the information processed by the University is done as part of fulfilling contractual purposes or undertaking public tasks (as introduced herein). An example of where consent will be sought is when the University asks PGR students, whether they wish for details of their graduation to be published in the media.

Where it is necessary to seek consent to process their personal data, this will be made clear to individuals at the point of data collection. Consent is optional. Individuals are under no compulsion to provide their consent, and where consent is provided, you will have the right to withdraw consent at any time, from which point the University's use of your personal data will stop.

For the avoidance of doubt, when signing to accept the terms and conditions of study at the University, the University ***is not*** asking PGR students for their consent to process personal data.

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, University policy or procedures primarily concerned with the protection of personal data may trigger an earlier review.

12 Availability

This Privacy Notice will be published on the University website, and copies will be provided to employees when they join the University.

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.