University of St Andrews

University Privacy notice: collection and use of employee personal data

Document type	**Policy**
Scope (applies to)	All staff
Applicability date	16/02/2018
Review / Expiry date	30/07/2023
Approved date	19/10/2022
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
EDI review/Equality impact assessment	None
Key terms	Information governance and management/Data protection/Privacy Information
Purpose	To advise people how their personal data are used by the University

Version number	**Purpose / changes**	**Document status**	**Author of changes, role and school / unit**	**Date**
4.0	Fourth version issued after periodic review	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	07/10/2022

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 UK 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") or a territory with no adequacy agreement 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 employees as to: how their personal data will be used by the University and relevant third parties in the context of their employment and when their employment ends; 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 within the context of employment.

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, email dataprot@st-andrews.ac.uk

4. **The purposes for which the University will make use of employees' personal data**
   The University may make use of an employee's personal data both during and after their employment 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.

5. **Communication**

Enabling persons within and outwith the University to identify and reach University employees

- Work-based contact details will be used by the University to enable persons within and outwith the institution to make contact with individuals in connection with their role at St Andrews.
    - This will include adding and making basic employee contact details, such as: name, place of work, telephone number and email address available in the University staff directory, the University electronic mail ("email") address book along with other directories/points of contact.

Directly engaging with people

- Work-based contact details 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 duties and to the services/facilities that are available to employees.
    - This will include providing employees with updates by email on what is happening across the University.

Use of personal contact details for disaster recovery or business continuity purposes

- The University will hold and may also make use of home/residence and other personal contact details to attempt to reach individuals as necessary to support day-to-day operations and to maintain the health, safety and wellbeing of the University community, specifically:
    - Home/residential contact details will be made available to other employees and/or agents of the University to enable persons to be contacted for the purposes of disaster recovery or business continuity.

6. **Complaint handling**

Assessment/investigation 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 students/members of the public.
- This may include concerns raised of bullying, harassment, discrimination and sexual violence raised via the University's '*Report and Support*' scheme.

Responding to investigations by the Ombudsman and other Regulators

- The development and submission of responses from the University, when responding to investigations undertaken by the Scottish Public Services Ombudsman ("the SPSO"), the Information Commissioner's Office ("the ICO") and any other Regulator with powers to investigate areas of the University's operation.

7. Employee relations

- The administration and execution of voluntary surveys of staff opinion – connected with the assessment and development of the staff experience and performance of the University.

8. 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. recruitment and promotion; 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. This is to carry out our obligations and exercise specific rights in relation to employment. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

9. Financial Management

Payroll administration

- Making salary and other contractual payments and processing statutory (e.g. tax and national insurance) payroll deductions.
- Making voluntary deductions e.g. cycle to work scheme payments.
- Managing expense claims and reimbursements.
  - This can include making details of expense claims available into the public domain, in response to requests for information, which require a response under freedom of information or environmental information legislation.
- Notifying employees of their employment-related tax liabilities.

Pension contribution management

- Administering payments of the institution's employers' and employees' contributions to pension schemes.

10. Governance

- Making senior officer appointments.
- Publication of University Senior Officer remuneration details in the University's Financial Reports.
- Management of elections for staff representatives on the University Court.
- Managing disclosures made to the University under public interest disclosure ("Whistleblowing") legislation.

11. Health and Safety Management

- Organising and reviewing inspections of the workplace and operations.
- Consultation with employees.
- Providing instruction and training.

    - This will include the review of training records to understand whether training gaps exist or otherwise.
- Hazard identification and risk assessment.
    - This will include risk assessment to understand if employees may be exposed to hazardous working environments/conditions and/or substances.
- Undertaking and reviewing workplace display screen equipment assessments.
- Maintaining records of exposure to hazardous substances/environment, including: noise; asbestos; ionising radiation; lead, etc.
- Incident management and reporting.
    - This will include accident reporting and review internally e.g. to a School/Service Health and Safety Committee and/or to an external regulatory or other authority e.g. the Health and Safety Executive.

12. Human Resource Management

Managing the contract of employment

- The creation and maintenance of a staff record.
    - This will include details of your home/residency and, if you so choose, details of next of kin.
- Recording details of an employee's recruitment and appointment.
    - This will include a record of the position as advertised and the associated terms and conditions, an individual's application for a position, including any references and other evidence e.g. records of qualifications, proof of entitlement to work in the United Kingdom.
- Recording details to make payments and taxable deductions, etc.
        - Bank details, National Insurance Number.
- Entitlement to work in the United Kingdom
    - Recording and retaining details, as set by the Home Office that evidence an entitlement to work in the UK.
- Probation.
    - Maintaining records of the establishment of probation objectives and associated monitoring and review.
- Performance management.
    - E.g. Annual career review, capability management.
- Training and development.
    - The organisation and delivery of training/staff development activities both at the University and in any other institution with which the University engages for providing such development.
- Recording and reviewing annual leave entitlements and any other authorised absence from work.
    - This may include: maternity leave; parental leave; research leave; sabbaticals; and attendance at external events.
- Managing academic and other promotions.
- Absence and return to work.
    - This may include recording/retaining details of a medical condition as described by a health care practitioner in a fitness to work note etc. and the review and consideration of those details, by a line manager and/or Human Resources when managing an employee's return to work etc.
- Disciplinary procedures.
    - Understanding and recording the facts surrounding a potential disciplinary issue and reaching a determination on matters, as per University policy and procedures.

- This may include the use of imagery captured via University operated Close Circuit Television ("CCTV") systems and/or other information gathered/created via (electronic) systems managed by the University, including access control (door entry) logs – to determine whether an employee(s) have complied with University policy/regulation and/or legislation.
- Assessment of any information provided by third parties – to determine whether an employee(s) have complied with University policy/regulation and/or legislation.
- The activities involved in conducting disciplinary proceedings concerning alleged/proven breaches of the institution's academic regulations or for misconduct. This may include communicating outcomes to third-parties, where a common law duty of care obligation on the University arises.

- Grievance process.
- Recording attendance/non-attendance during industrial action.

Workforce planning

- Analysing the size, composition, structure and competencies of the University's workforce; reporting on the composition of the institution's workforce to regulators; developing role (job) descriptions; and conducting role evaluations to assign roles to grades/bands in a salary structure.

13. 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.

14. Information and Communications Technology ("ICT") Management

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.

ICT systems development and testing

- The University may also, where required, use copies of elements of the personal data of staff 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.

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.

15. 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.

16. 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 training records and other records/documentation held by the University to pursue or defend a claim.

17. Media Management

- Media communications.
    - e.g. Issuing press releases on University activities and responding to media inquiries.
- Personal data may also be shared where it is necessary for the University to respond to a right of reply where there is an intention to publish a media article and it is I the public interest to respond to claims made.
- Publishing details of staff involvement in University activities via the institution's website and other publications.

18. Public Safety

- Images captured by CCTV systems operated by or on behalf of the University will be used for the purposes of providing a safe campus environment and for the prevention and detection of crime.

19. Research

Administering research income

- Agreeing to the terms and conditions of funding; monitoring the use of funds and ensuring compliance with terms and conditions of funding; preparing reports and other information on the use of funds for funding providers.

Research planning and design

- Defining project roles and responsibilities; securing necessary ethical reviews and regulatory approvals; determining requirements for project resources; preparing research proposals.

Research publications and outputs

- Planning and preparing content (commissioning, research, writing, editing) for publication; designing publications; producing publications.
- Making research publications available via institutional and other repositories.
- Making research activities, research impact case studies and outputs accessible, via Websites, aggregation of (open) metadata, etc.
- Citation analysis of publications.

Research quality

- Conducting internal reviews of research quality and standards; facilitating and participating in external reviews of research quality and standards (e.g. Research Assessment Framework).

20. 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.

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).

22. Support Services

- Providing and administering access to services and facilities provided by or through the University as necessary to support employment 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;
    - Production of a University staff identity card, which provides access to buildings and other facilities such as printing;
    - 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;
    - Car parking permits; and
    - Managing requests for services from Estates such as requests for repairs to University buildings and maintaining records of the request and the work completed (job cards).

23. Teaching, learning and assessment

- The organisation and delivery of teaching and learning, and assessment. This may include face-to-face and on-line delivery.

24. University Archive

- Core elements of the staff 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 staff body over time.

25. 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 bases that the University will rely upon for the lawful processing of employee personal data for the purposes/activities introduced, above, are outlined below.

- **Contract or preparation for entry into a contract**
  - In this context, the contract of employment between an employee and the University i.e. –
    - The majority of the personal data that the University collects (or creates) from both prospective and current employees is used by it so that it can provide access to a range of services and facilities that are consistent with supporting the contract of employment. For example, on accepting an offer of employment, the University will ask for bank details so that salary and other payments can be made. The use of those details is consistent with the University meeting its contractual obligations (payment).

- **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 HMRC, making returns to UK and European funding bodies and retaining evidence of proof of entitlement to work 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.
    - For example, the Universities (Scotland) Act 1889 c. 55, Section 6, Paragraph 1 i.e. "[Powers of the University Court] To administer and manage the whole revenue and property of the University." Where the University is required to use personal data to account for monies and/or other University resources, it can rely on the authority from the said legislation as a legal basis to do so. An example would include maintaining details of equipment issued to an employee, so that the return of those items can be managed, when a person leaves or changes their job; and
    - 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 making staff (work) contact details available.

- **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 member of staff where they had lost consciousness.

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

Within the University

In order to meet its contractual obligations with employees and management responsibilities i.e. those necessary to support and sustain operation of the University and statutory requirements, the University will share employee personal data across Schools and Services. For example, HR Services will advise IT Services when employees join and leave the University, so that access to services such as email can be managed.

27. Outwith the University

The University may disclose certain personal data to external bodies as categorised below. At all times, the nature and 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
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, which is provided by the Microsoft Corporation and accommodation and travel services, brokered through DP&L. 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 the relevant parties which: o 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 o 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.
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.
Government agencies and local authorities, with statutory powers to obtain information from the University as a higher education institution	For example, the Child Support (Information, Evidence and Disclosure) Regulations 1992 gives the Child Maintenance Service power to require information about salary, pension and tax contributions from employers.

and/or an employer.	
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.
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 work 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 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 at work and has been taken to hospital for treatment.
Partner institutions	The University will share personal data of employees whose duties require that they work with partner institutions as necessary to manage and administer that individual's work with the University and that body.
Recognised Trade Unions	The University may pass on to recognised trade unions, the contact details of individuals who have recently taken up employment with the University, so that a trade union may make initial contact to inform individuals about the services provided by them.
References	The University may release personal information concerning a current or former member of staff to a third party in response to a request for a reference when it has the prior consent of the individual concerned, or where the transfer is necessary to progress a contract to which an individual is subject or where it is found to be in the legitimate interests of an individual. While such references typically concern the recruitment process for employment, this may also include confirming details of an individual's employment and/or earnings in response to requests for mortgages from lenders, or to progress a rental agreement etc.
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.
Research bodies/funders	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.
The Equalities Challenge Unit	To support reporting requirements allied with the Athena SWAN charter.
The public	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 and annual financial reports. Information on the University's activities and work, which staff are involved in may also be made available via the University Website and University publications.
Universities Superannuation Scheme ("USS") and the University of St Andrews Superannuation and Life Assurance Scheme ("SLAS")	Personal data is passed to pension fund trustees, as required for the provision of pensions by those providers.

28. Details of transfers of personal data to countries outwith the EEA

Where a University employee is working overseas 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.

Where a University employee works overseas, and is paid in local currency, the University may transfer to the local tax authority or to a third party in-country agent such as a payroll service provide, details of employment that employment, so that arrangements can be made to collect local duties.

29. 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 employees during the duration of their employment and for up to six years following the end of their contract with the University, after which time elements of the staff 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, 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.

30. 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.

31. 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 employees 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 i.e. the contract of employment. An example of where consent may be required is when a member of staff seeks Occupational Health services.

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 employment the University ***is not*** asking employees for their consent to process personal data.

32. 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/

33. 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 employment, circumstances can arise where an individual has an obligation either under law, or via the contract of employment 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 salary 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 employment, then action under University disciplinary policy may arise, which could lead to dismissal.

- Inability to provide proof of the entitlement to work in the UK, may impact negatively on the University's ability to employ.

34. 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.

35. 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.

36. 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.

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	16/02/2018
2.0	Second version (periodic review)	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	14/05/2019
3.0	Periodic review (minor changes made – reference to Report and Support and use of Data for ICT testing)	Approved	C Milne, Head of Information Assurance and Governance, Office of the Principal	08/09/2021