EMPLOYEE DATA PROTECTION POLICY

This document sets out the University of St Andrews Students' Association ('the Students' Association') policy on the protection of information relating to staff members, temporary or casual workers, contractors and volunteers. Protecting the confidentiality and integrity of personal data is a critical responsibility that the Students' Association takes seriously at all times. The Students' Association will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR)

KEY DEFINITIONS

Data processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Personal data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Students' Association possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive personal data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

PRIVACY NOTICE

This policy, together with the information contained in the table of staff member data appended to the policy, constitutes a privacy notice setting out the information the Students' Association holds about staff members, the purpose for which this data is held and the lawful basis on which it is held. The Students' Association may process personal information without staff members' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about staff members should change, the Students' Association will update the table of staff member data with the new purpose and the lawful basis for processing the data and will notify staff members.

FAIR PROCESSING OF DATA

Fair processing principles

In processing staff members' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Students' Association will use personal information in the following circumstances:

- when it is needed to perform staff members' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the Students' Association's legitimate interests (or those of a third party) and staff members' interests and fundamental rights do not override those interests.

The Students' Association may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect staff members' interests (or someone else's interests); or
- when it is necessary in the public interest [or for official purposes].

Lawful processing of sensitive personal data

The Students' Association may process special categories of personal information in the following circumstances:

- in limited circumstances, with explicit written consent obtained from the data subject;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring [or in relation to membership of the University of St Andrews occupational pension schemes offered by the Students' Association]; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Students' Association may process this type of information where it is needed in relation to legal claims or where it is needed to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where a staff member has already made the information public. The Students' Association may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;

- information about staff members' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;

- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and

- Information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment law obligations.

Lawful processing of information about criminal convictions

The Students' Association envisages that it will hold information about criminal convictions. If it becomes necessary to do so, the Students' Association will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the Students' Association's obligations. Less commonly, the Students' Association may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where the staff member has already made the information public.

The Students' Association will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, the Students' Association will collect information about criminal convictions as part of the recruitment process or may require staff members to disclose information about criminal convictions during the course of employment.

Consent to data processing

The Students' Association does not require consent from staff members to process most types of staff member data. In addition, the Students' Association will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If a staff member fails to provide certain information when requested, the Students' Association may not be able to perform the contract entered into with the staff member (such as paying the staff member or providing a benefit). The Students' Association may also be prevented from complying with legal obligations (such as to ensure the health and safety of staff members).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, staff members may be asked for written consent to process sensitive data. In those circumstances, staff members will be provided with full details of the information that is sought and the reason it is needed, so that staff members can carefully consider whether to consent. It is not a condition of staff members' contracts that staff members agree to any request for consent.

Where staff members have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once the Students' Association has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law. In such circumstances any other identified legitimate basis will be communicated to staff members.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

The Students' Association does not envisage that any decisions will be taken about staff members using automated means, however staff members will be notified if this position changes.

The Students' Association is classified as a data controller and a data processor. We must maintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling and processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of our members, guests or customer. If we at any point determine the purpose and means of processing out with the instructions of the members, guests or customer, we shall be considered a data controller and therefore breach our contract with the member, guest or customer and have the same liability as the member, guest or customer. As a data processor, we must:

- Not use a sub-processor without written authorisation of the customer
- Co-operate fully with the ICO
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the customer of any personal data breaches

If you are in any doubt about how we handle data, contact the DPL (Data Protection Lead) for clarification.

Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Where relevant, ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Providing data protection training to all of our staff

Your responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay to the DPL

COLLECTION AND RETENTION OF DATA

Collection of data

The Students' Association will collect personal information about staff members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. The Students' Association may sometimes collect additional information from third parties including former employers or other background check agencies such as the Scottish Government for the purposes of the Protection of Vulnerable Groups (PVG) scheme. The table of staff member data appended to this policy relates to information which is collected at the outset of employment. From time to time, the Students' Association may collect additional personal information in the course of job-related activities throughout the period of employment. If the Students' Association requires to obtain additional personal information, this policy will be updated or staff members will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

Retention of data

The Students' Association will only retain staff members' personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the table of staff member data appended to this policy.

When determining the appropriate retention period for personal data, the Students' Association will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether the Students' Association can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances the Students' Association may anonymise personal information so that it can no longer be associated with individual staff members, in which case the Students' Association may use such information without further notice to staff members. After the data retention period has expired, the Students' Association will securely destroy staff members' personal information.

DATA SECURITY AND SHARING

Data security

The Students' Association has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are are summarised below:

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice, complying with the Students' Association's policies and procedures and the data protection legislation;
- everyone managing and handling personal information is appropriately trained to do so and appropriately supervised;
- paper files are kept appropriately secure and ICT security protocols and procedures are followed fully by all staff;
- personal data is not shared outside of the Students' Association without appropriate consent and only where it is compliant with the Privacy Notice in place at the time the data was collected;
- systems will be configured in a way which enables them to allow individuals to exercise their rights (as stated below);
- queries about handling personal information are promptly and courteously dealt with;
- a regular review is made of the way personal information is managed;
- confidential paper records are securely disposed of within the terms of the Students' Association's data retention policy;
- redundant ICT equipment is recycled using the services of a University of St Andrews approved contractor who sanitises all hard drives in a secure manner; and
- staff laptops and other mobile devices are encrypted; and
- methods of handling personal information are regularly assessed and evaluated.

Access to personal information is limited to those staff members, agents, contractors and other third parties who have a business need to know. They will only process personal information on the Students' Association instructions and are subject to a duty of confidentiality. The Students' Association expects staff members handling personal data to take steps to safeguard personal data of staff members (or any other individual) in line with this policy.

Data sharing

The Students' Association requires third parties to respect the security of staff member data and to treat it

in accordance with the law. The Students' Association may share personal information with third parties, for example the University of St Andrews in the context of the membership of the occupational pension schemes provided by the University. The Students' Association may also need to share personal information with a regulator, such as the Office of the Scottish Charity Regulator (OSCR), or to otherwise comply with the law.

The Students' Association may also share staff member data with third-party service providers where it is necessary to administer the working relationship with staff members or where the Students' Association has a legitimate interest in doing so. The following activities are carried out by third-party service providers:

- payroll and pension administration: the University of St Andrews

Transfer of data outside the EU

Personal information is processed by our staff, or in the case of payroll and pension data the University of St Andrews staff, in St Andrews, Scotland. Neither the Students' Association or the University of St Andrews will transfer staff members' personal information outside of the UK.

STAFF MEMBER RIGHTS AND OBLIGATIONS

Accuracy of data

The Students' Association will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Staff members are under a duty to inform the Students' Association of any changes to their current circumstances. Where a staff member has concerns regarding the accuracy of personal data held by the Students' Association, the staff member should contact the HR Manager to request an amendment to the data.

Staff member rights

Under certain circumstances, staff members have the right to:

- **Request access** to personal information (commonly known as a "data subject access request").
- **Request erasure** of personal information.
- **Object to processing** of personal information where the Students' Association is relying on a legitimate interest (or those of a third party) to lawfully process it.
- **Request the restriction of processing** of personal information.
- **Request the transfer** of personal information to another party, e.g. a new employer.

If a staff member wishes to make a request on any of the above grounds, they should contact the HR Manager in writing. Please note that, depending on the nature of the request, the Students' Association may have good grounds for refusing to comply. If that is the case, the staff member will be given an explanation by the Students' Association.

Data subject access requests

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

The Students' Association may need to request specific information from the staff member to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person

who has no right to receive it.

COMPLIANCE WITH THIS POLICY

The Students' Association's responsibility for compliance

The Students' Association has appointed a Data Protection Lead (DPL) [need to determine who this will be] who is tasked with overseeing compliance with this policy. If staff members have any questions about this policy or how the Students' Association handles personal information, they should contact the DPL. Staff members have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO can be contacted at:

Information Commissioner's Office – Scotland
45 Melville Street
Edinburgh
EH3 7HL

Telephone - 0303 123 1115

Email - Scotland@ico.org.uk

Data security breaches

The Students' Association has put in place procedures to deal with any data security breach and will notify staff members and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

In certain circumstances, the Students' Association will be required to notify the ICO of a data security breach within 72 hours of being made aware of the breach. Therefore, if a staff member becomes aware of a data security breach it is imperative that they report it to the Management Accountant / General Manager immediately who will in turn notify the DPL.

Privacy by design

The Students' Association will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as "privacy by design").

Training

All staff will receive training on this policy. New staff will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or of our policy and procedures. Staff involved in significant data processing activities and processing of sensitive data will receive refresher training annually.

Training will be delivered through a mix of in-house team meetings or via the suite of online training modules which are available to all staff.

It will cover:

- The applicable law relating to data protection

- Our data protection and related policies and procedures, including our privacy notice.

Completion of training is compulsory. If you require additional training on data protection matters, contact the DPL.

Staff members' responsibility for compliance

All staff members, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Staff members should observe, as a minimum, the following rules:

- Staff members must observe to the letter any instruction or guidelines issued by the Students' Association in relation to data protection.
- Staff members should not disclose personal data about the Students' Association, colleague or third parties unless that disclosure is fair and lawful, in line with this policy;
- Staff members must take confidentiality and security seriously, whether the staff member considers the information to be sensitive or not.
- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay.
- Staff members must not make any oral or written reference to personal data held by the Students' Association about any individual except to other staff members who need the information for their work or an authorised recipient.
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information.
- If a staff member is asked by an unauthorised individual to provide details of personal information held by the Students' Association the staff member should ask the individual to put their request in writing and send it to the DPL. If the request is in writing the staff member should pass it immediately to their line manager **OR** DPL.
- Staff members must not use personal information for any purpose other than their work for the Students' Association.
- If a staff member is in doubt about any matter to do with data protection they must not refer the matter to their line manager **OR** DPL immediately.
- Passwords should not be disclosed and should be changed regularly.
- Staff members or third party personal data should not be left unsecured or unattended, e.g. on public transport.
- Unauthorised use of or access to computer equipment provided by the Students' Association is not permitted.
- Staff members must ensure that all confidential information, whether containing staff member or third party personal data or not, is secured when it is not in use or when the staff member is not at work.
- Where remote or mobile working is permitted, staff members may use only encrypted equipment to carry out work and must ensure that devices are password protected and locked when not in use and must not store any staff member or third party personal data locally on their device.
- Emails containing staff member or third party personal data must not be sent to / from an external web-based email system.
- As far as possible, staff members or third party personal data contained in emails and attachments should be annonymised before it is sent by email; and
- Documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.
- Or use is made of an approved secure document exchange portal.

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.

DECLARATION

I confirm that I have received a copy of this policy and that I have read and understood it.

Name: _____

Signature: _____

Date: _____

STAFF MEMBER DATA						
Type of personal data	**Sensitive data?**	**Purpose of processing**	**Potential transfer to third parties**	**Lawful basis for processing**	**Grounds for processing sensitive personal data**	**Retention period**
Contact details	No	Administering the employment contract	HMRC / Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Date of birth	No	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Gender	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Marital status	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Information about race	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Information about ethnicity	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Information about religious beliefs	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Information about sexual orientation	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Information about political affiliations	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Next of kin / emergency contact	No	Safety and security	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	During employment
NI number	No	Payroll	HMRC / University / pension providers	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Salary information	No	Payroll	HMRC / University / Pension company	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Bank details	No	Payroll	HMRC / University	Legal obligation / Performance of contract / Legitimate interests	N/A	6 months post-employment
Tax details	No	Payroll	HMRC / University	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Pension details	No	Payroll / liaising with pension providers	HMRC / University / pension providers	Legal obligation / Performance of contract / Legitimate interests	N/A	75 years post-employment
Benefits information	No	Providing benefits to staff members	Benefit providers / University	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Driving license	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
CV	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Right to work documents	Yes	Checking right to work in the UK	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	2 years post-employment

STAFF MEMBER DATA						
Type of personal data	**Sensitive data?**	**Purpose of processing**	**Potential transfer to third parties**	**Lawful basis for processing**	**Grounds for processing sensitive personal data**	**Retention period**
Sick leave period of absence	No	Managing absence	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Performance details	No	Managing performance	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Qualifications	No	Making recruitment decisions / ascertaining ability to work	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Employment history	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Information about disability	Yes	Managing staff / health and safety requirements / ascertaining fitness to work	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-employment
Training records	No	Education, training and development requirements	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Professional memberships	No	Education, training and development requirements	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Disciplinary and grievance information	No	Staff management	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
CCTV footage	No	Safety, security, prevention and detection, identification and prosecution	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Information about use of IT systems	No	Ensuring network and data security / staff management	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	N/A	6 years post-employment
Photographs	No	Safety and security	N/A	Legal obligation / Performance of contract / Legitimate interests	N/A	During employment
Trade union membership	Yes	Deducting trade union fees	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	6 years post-employment
Health records	Yes	Managing absence / ascertaining fitness to work	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	6 years post-employment
Criminal convictions and offences	Yes	Making decisions about recruitment / continued employment	Professional advisors	Legal obligation / Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	6 years post-employment