Data Protection & Information Security Handbook

Approved by:	Board of Trustees	Date:	18 November 2019
Implementation date:	November 2019		
Review date:	November 2020		
Manager responsible:	Chief Executive Officer		

Contents

Data Protection & Information Security Policy

Introduction

The Falmouth & Exeter Students' Union (The SU) is committed to the protection of the personal data of students, employees and other individuals whom it holds information about.

The SU recognises the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and the Privacy of Electronic Communications Regulations (PECR) as the primary statutory responsibilities relating to data handling and processing.

To this end, every individual employee handling data collected or administered by The SU must take responsibility and due consideration for its appropriate use in line with this policy and the declared processing activities.

These arrangements apply to all employees and volunteers, and are overseen by The SU's senior management team and Chief Executive Officer. Any deliberate breach of this policy may lead to disciplinary action being taken, or access to The SU's facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Chief Executive Officer.

Purpose

The SU is registered with the Information Commissioner to process 'personal data' and is named as a data controller under the register kept by the Information Commissioner in accordance with GDPR as enacted by the DPA.

The SU holds and processes information about employees, students, and 'other data subjects' for academic, administrative and commercial purposes. In addition, The SU may be required by law to collect and use information in order to comply with the requirements of central government.

The DPA regulates the way that we handle 'personal data' that we collect in the course of carrying out our functions and gives certain rights to people whose 'personal data' we may hold. All staff or others, who process or use any 'personal data', must handle the data properly under the DPA.

The SU is committed to protecting the rights and freedoms of individuals in accordance with the provisions of the DPA. This document aims to outline the responsibilities of The SU, its staff and members, relating to the collection, use and disclosure of data and the rights of the data subject to have access to 'personal data' concerning them.

Scope

This policy is applicable to all staff and students of The SU and to those who in the course of their duties may be party to information held by The SU (e.g. Students/Casual Staff, external contractors, agency staff, and seasonal workers) together with the data subjects themselves.

This policy does not apply to Falmouth Exeter Plus, Falmouth University or to the University of Exeter, which are separate Data Controllers.

Information covered by the DPA

The DPA uses the term 'personal data'. For information held by The SU, personal data means any recorded information held by The SU and from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details. It will include any expression of opinion about a living individual or any indication of The SU's intentions about that individual.

Data Protection Principles

The SU will comply with the six enforceable data protection principles by making sure that personal data is:

1. Lawfully, fairly and transparently processed;
2. Processed for specified, explicit purposes;
3. Adequate, relevant and limited to only what is necessary;
4. Accurate and kept up to date;
5. Not kept longer than necessary; and
6. Processed in handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage.

Definitions

'Staff', 'students', 'other data subjects' and 'third parties' may include members of the public, current, past and prospective employees and students, funded bodies, suppliers, contractors, contracts, referees, friends or family members.

'Processing' refers to any action involving personal data including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

Conditions for processing personal and sensitive personal data

Before processing any personal data, The SU will ensure that at least one of the following conditions is met:

1. The individual has consented to the processing;
2. The processing is necessary for the performance of a contract with the individual;
3. The processing is required under a legal obligation (other than one imposed by a contract);
4. The processing is necessary to protect vital interests of the individual;
5. The processing is necessary to carry out public functions e.g. administration of justice;
6. The processing is necessary in order to pursue our legitimate interests or those of third parties (unless it is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject).

Sensitive personal data includes information about racial or ethnic origin, political opinions, religious and other beliefs, trade union membership, genetics, biometrics or health condition, sex life or orientation, criminal proceedings or convictions.

Under the DPA, one of a set of additional conditions must be met before processing 'sensitive personal data'. Therefore, The SU will ensure that one of the following additional conditions is met before processing any sensitive personal data:

1. The individual has freely given, specific, informed consent to the processing;
2. The SU is required by law to process the information for employment purposes;
3. The SU needs to process the information in order to protect the vital interests of the individual or another person - for example in a medical or personal safety emergency; and
4. The processing is necessary to deal with the administration of justice or legal proceedings.

Individuals' rights

The SU will ensure that individuals' rights under the DPA are met. Those rights include:

1. The right to withdraw consent to processing;
2. The right to obtain their personal information ("a Data Subject Access Request" (DSAR)) from us except in limited circumstances;
3. The right to ask us not to process personal data where it causes substantial unwarranted damage to them or anyone else;
4. The right to claim compensation from us for damage and distress caused by any breach of the DPA.

Notification of data held

The SU shall notify all staff and students and other relevant data subjects of the types of data held and processed by the SU concerning them, and the reasons for which it is processed.

The information which is currently held by The SU and the purposes for which it is processed are set out in the SU's suite of Privacy Notices.

When The SU introduces processing for a new or different purpose, it will amend the relevant privacy Notice(s) accordingly.

Legal requirements

The SU may be required to disclose staff or student user data by a court order or to comply with other legal requirements. Unless legally restricted from doing so, the SU will use all reasonable endeavours to notify those concerned in advance

No commercial disposal to third parties

Save as described above or with prior permission from the individual(s) concerned, The SU shall not sell, rent, distribute or otherwise make user data available commercially to any third party.

Staff responsibilities

All staff shall:

1. Ensure that all personal information that they provide to The SU in connection with their employment is accurate and up-to-date;
2. Inform the relevant department or The SU's Chief Executive Officer of any changes to information - for example, change of address; and
3. Check the information that The SU shall from time-to-time make available in written or automated form, and inform the relevant department or The SU's Chief Executive Officer of any errors or, where appropriate, follow procedures for amending entries on computer systems.

The SU shall not be responsible for errors of which it has not been informed. However, to minimise instances where personal data may be inaccurate or out of date, The SU will aim to contact staff regularly for the purpose checking data accuracy (normally annually as part of the Personal Development Review process).

When staff hold or process information about students, colleagues or other data subjects (for example, students' pastoral files, references or details of personal circumstances), they are responsible for following good data protection practice including ensuring that:

- All personal information is kept securely and up to date; and
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

Unauthorised disclosure may be a disciplinary matter and, in some circumstances, may constitute gross misconduct.

When staff supervise work colleagues or students undertaking work which involves the processing of personal information, they must ensure that those members of staff or

students are aware of this Policy and the Data Protection Principles and, in particular, the requirement to obtain the data subject's consent where appropriate.

The SU Directors

The SU Directors must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the frameworks agreed and following the guidance set out in the Data Protection and Information Security Handbook.

The SU Directors are required to conduct six monthly audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

Student responsibilities

All students shall:

1. Ensure that all personal information that they provide to The SU in connection with their employment is accurate and up-to-date;
2. Inform the relevant department or The SU's Chief Executive Officer of any changes to information - for example, change of address; and
3. Check the information that the SU shall from time-to-time make available in written or automated form, and inform the relevant department or The SU's Chief Executive Officer of any errors or, where appropriate, follow procedures for amending entries on computer systems.

The SU shall not be responsible for errors of which it has not been informed.

Information Security

Data Storage
All electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by the SU employees or staff, in accordance with statutory, regulatory, contractual, and the SU Policy requirements.

The SU has the following platforms for securely storing data online – SharePoint, Compass Online and the user's personal U Drive. The SU staff and volunteers must store data they handle on one of these platforms only - as detailed within the Data Protection and Information Security Handbook.

The SU recognises that from time-to-time staff and volunteers may need to remove restricted information, including personal data and confidential information, from the SU premises (for example, when travelling between campuses). In those circumstances:

- Information processed on portable devices and media must be encrypted or password protected using a password that is not stored with the device.

- It is the member of staff and/or volunteer's responsibility to taker the utmost care so as to avoid loss of data held in a physical form.

Third Party Contracts
From time-to-time, the SU enters into contracts with third parties leading to a transfer of personal data to those third parties. Prior to any data transfer, SU staff shall ensure that the SU's contract with the third party includes provisions designed to ensure the parties' compliance with the prevailing data protection legislation.

IT Systems and equipment
All SU staff must undertake data protection and information security training to ensure sufficient security awareness.

At all times and in all locations, SU staff and volunteers must secure digital equipment and media against theft, loss or unauthorised access.

Where possible, SU staff should access all work-related IT systems through the VDI system only, including when working remotely.

In addition, all digital equipment and media must be disposed of securely and safely when no longer required - the Data Protection and Information Security Handbook outlines the appropriate procedures.

Rights to Access Information

Staff, students and other data subjects in The SU have the right to access any personal data held about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a Data Subject Access Request ("DSAR") request in writing to the SU's Penryn Campus Office.

Currently, The SU does not make a charge for DSARs, but reserves the right to charge where the request is manifestly unfounded or excessive when it may charge a reasonable fee for the administrative costs of complying with the request.

The SU may also charge a reasonable fee if an individual requests further copies of their data following a request. This fee will be based on reproduction and administrative costs of providing further copies.

The SU aims to comply with requests for access to personal information as quickly as possible and, unless there is good reason, within one month. When the SU exceeds the period of one month, it will provide the relevant data subject with a written explanation for the delay.

Policy Monitoring

Day-to-day responsibility for compliance with this Policy and its related policies and procedures rests with the SU's Chief Executive Officer and Senior Management Team.

The Chief Executive Officer is responsible for ensuring that the Policy is reviewed annually or sooner should the need arise.

The Data Controller and the Registered Data Protection Officer

The SU is the data controller under the Act, and the SU's Chief Executive Officer is ultimately responsible for implementation. Currently responsibility for day-to-day matters is with the Chief Executive's nominee, Richard Scrase (Advice Service Director). Information and advice about the holding and processing of personal information is available from Richard Scrase.

Retention of data

The SU will keep different types of information for different periods of time, depending on legal, academic and operational requirements. A detailed Retention Schedule Guidance document is attached to this document (see Annex A). Further information and advice about the recommended retention periods is available from the SU's Penryn Campus Office.

Compliance and commitment

Compliance with the DPA is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the SU's Chief Executive Officer or their nominee - contact details are at the end of this document.

Any individual who considers that the SU has breached or deviated from this Policy's provisions and in so doing infringed their data rights should raise the matter with the SU's Chief Executive Officer or their nominee. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

The SU is committed to protecting the rights and freedoms of individuals in accordance with the provisions of the DPA and as part of that commitment will ensure that:

- Everyone managing and handling personal information understands that they are responsible for following good data protection practice;
- There is someone with specific responsibility for data protection in the organisation;
- Staff who handle personal information are appropriately supervised and trained;
- Queries about handling personal information are dealt with promptly and courteously;
- Individuals know how to access their own personal information;
- Methods of handling personal information are assessed and evaluated regularly;
- Any disclosure of personal data will comply with approved procedures;
- All necessary steps are taken to ensure that, at all times, personal data is kept secure against unauthorised or unlawful loss or disclosure; and

- All contractors to whom the SU supplies personal information confirm that they will observe the requirements of the DPA with regard to that personal information.

Further Information

For further information and guidance on this policy and working with the Data Protection Act 2018, please follow this link to Privacy & Data Protection or contact the SU's Chief Executive Officer:

Falmouth and Exeter Students Union
Penryn Campus,
Treliever Road
Penryn
TR10 9FE

T: 01326 255861

E: dataprotection@thesu.org.uk

Further information is also available from:

- The Information Commissioner
  www.ico.org.uk

- The Ministry of Justice (formerly The Department of Constitutional Affairs)
  www.justice.gov.uk

Data Retention Policy

1. Introduction

Falmouth & Exeter Students' Union ('the SU') holds a great deal of important information that is crucial to the running of the organisation. Data we hold must be available and accessible and usable on demand by an authorised entity. It is important that any personal data is securely erased or anonymised when the purposes for which it is kept no longer exist, in order to comply with the general data Protection Regulation (GDPR).

2. Scope

The Data Retention Policy applies to data held by all members of the SU staff[1] regardless of the form in which it is held. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.

The policy applies to all members of the SU staff who are given access to data held by the SU. It includes all devices including removable media/portable devices, and paper-based records.

With regard to electronic systems, it applies to use of the SU owned facilities and privately/externally owned[2] systems when connected to the SU network directly or indirectly. The policy applies to all the SU owned/licensed data and software, be they loaded on the SU or privately/externally owned systems, and to all data and software provided to the SU by sponsors or external agencies.

3. Policy awareness and guidance on data protection

The Data Retention Policy will be made available to the SU staff in the Data Protection & Information Security Handbook.

4. Disposal of Information

The SU staff have an obligation to dispose of personal, confidential and business critical information in a secure manner. This includes ensuring that all backups and copies are included in the destruction of records.

Please refer to the retention Schedule at the bottom of this document to find out how long certain types of data are to be retained. Changes to the Schedule are at the discretion of the SU's Chief Executive Officer and do not require Trustees' approval.

5. Legal and contractual requirements

The SU will abide by all relevant legislation related to the holding and processing of information. In particular, data protection legislation defined as; (i) unless and until the

[1] For the purpose of this policy, 'SU staff' includes staff employed by SU directly or through Falmouth University

[2] 'Owned' is deemed to include leased, rented or on-loan

GDPR is no longer directly applicable in the UK, the General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

6. Responsibilities

The SU's Chief Executive Officer is responsible for the Data Retention Policy.

The SU staff are responsible for ensuring that information used is managed and used in accordance with the Data Retention Policy.

Any member of the SU staff who is concerned around data retention should report to their line manager or the Chief Executive Officer.

7. Third party contractors

The SU should have appropriate contracts with third parties who are storing, processing or transmitting data covered by this policy so that the applicable retention period is adhered to.

8. Maintenance

The Data Retention Policy will be monitored and maintained and reviewed at least annually and whenever a significant event occurs which requires its revision. The SU should also regularly audit and monitor its approach to the secure disposal of data.

Retention Schedule

Type of record	Retention period
Staff	
Personnel files of employed and volunteer staff including training records and notes of disciplinary and grievance hearings	6 years from the end of employment
Application forms/interview notes for paid and volunteer staff	6 months from the date of the job advertisement
Facts relating to redundancies	6 years from the date of redundancy
Payroll records, Income Tax and NI Returns, including correspondence with tax office	3 years after the end of the tax year to which the records related
Statutory Maternity and adoption Pay records and calculations	3 years after the end of the tax year in which the maternity period ends
Statutory Sick Pay records and calculations/Sickness records	Three years after the end of each tax year for Statutory Sick Pay purposes
Individual pension entitlement and contribution history	As long as there is a member or dependant liability
DBS checks for staff and volunteers	6 years after end of employment
Accident books, and records and reports of accidents	3 years after the date of the last entry
Health Records for staff and volunteers	During employment/ volunteer engagement
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years
Examination, testing, monitoring and control records:	Review 5 years after last action
Health and Safety Training, guidance and instructions: Risk assessment reports and reviews:	Review 3 years from date superseded The HSE recommends 40 years for personal records http://www.hse.gov.uk/health-surveillance/record-keeping/index.htm
Contractual records	6 years

References received for staff	1 year
Annual leave records	2 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given information to enable references to be provided	5 years from reference/ end of employment
Summary of record of service eg: name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years
Advice Service	
Case files records	7 years
Emails (other than those held within case files)	12 months: 31 July in the following generation of the email
Student Opportunities	
Club and Societies memberships	12 months: 31 July in the year following leaving university
Student Voice	
Sabbatical officer nominations	12 months after elections
Committee nominations	12 months after elections
Committee members	12 months after end of term of office
Course representative nominations	12 months after elections
Course representatives	12 months after end of term of office
Central Services	
Financial records	7 years
Student driver records	1 September immediately following end of the academic year
Emails	12 months: 31 July in the following generation of the email

Students Privacy Notice

Introduction

Falmouth & Exeter Students' Union ('the SU') is a data controller and is committed to protecting your personal data and working in accordance with all relevant data protection legislation.

This privacy notice explains how the SU processes and uses the personal data we collect from and/or in relation to its student members.

Developing a better understanding of our members through your personal data allows us to make better decisions, communicate more efficiently and, ultimately and help us to reach our goal of having a positive impact on every University of Exeter (Cornwall Campus) and Falmouth University student.

Where we collect information about you

The SU may hold data relating to you from a number of sources.

Data you provided to your University
Some of the data we hold on students is data that you provided to your University[3], either before you commenced your studies or during your time as a student and which, in turn, the University has provided to us[4].

Data you provided to the SU direct
This may include any forms you complete for us, documents including medical evidence/diagnosis of a disability, study needs assessment reports, appointment details, phone calls and emails.

Social Media
Depending on your settings or the privacy policies for social media and messaging services like Facebook, WhatsApp or Twitter, you might give us permission to access information from those accounts or services.

Information available publicly
This may include information found in places such as Companies House and information that has been published in articles/ newspapers.

When we collect it as you use our website
Like most websites, we use "cookies" to help us make our site – and the way you use it – better. Cookies mean that a website will remember you. They are small text files that sites transfer to your computer (or other digital device). They make interacting with a website faster and easier – for example, by automatically filling your name and address in text fields.

[3] i.e. University of Exeter or Falmouth University
[4] The SU has data sharing agreements with each of the University of Exeter and Falmouth University. To request a copy of those agreements, email the SU at dataprotection@thesu.org.uk

In addition, the type of device you use to access our website and the settings on that device may provide us with information about your device, including what type of device it is, what specific device you have and what operating system you are using. Your device manufacturer or operating system provider will have more details about what information your device makes available to us.

What personal data we collect and how we use it

Our records may include:

- Personal Identifiers and biographical Information – for example your student ID number and your date of birth
- Contact details – for example your address, email address and telephone number
- Sensitive personal data -for example, information about a disability
- Dates of meetings held with you
- Family details – for example details of other family members with whom you have given us consent to liaise

In addition, when you attend an event, join a student group or use one of our services the SU may ask for additional information such as:

- Your bank details to facilitate payments
- Information relating to your health - if you are taking part in a high-risk activity

Primarily, the SU will use your data to:

- Provide you with the services, products or information you asked for
- Administer your membership
- Keep a record of your relationship with us
- Ensure we know how you prefer to be contacted
- Understand how we can improve our services, products or information

The Student Opportunities Team uses your data in relation to your participation in the SU's various clubs and societies. Examples include:

- Administering your membership
- Arranging and administering relevant affiliations
- Facilitating your participation in events and activities
- Supporting the administration of your club or society

The SU may communicate with you by telephone, text, email, post or other electronic means.

The SU also collects routine statistical information about student participation in elections, committees, clubs, societies and other activities, which is later anonymised and analysed for audit and evaluation purposes. This information may subsequently be summarised and interpreted in the SU reports. The SU will take care is taken to ensure no individually identifiable information is disclosed.

Who we share your personal data with

Save for the exceptions listed below, other than with your written authority the SU will not disclose your personal data to third parties. You may be asked to sign a 'Consent to Liaise' form, on which you confirm whom we may or may not contact. In other instances, you may be asked to email us with the name of the person with whom you wish us to liaise.

We may need to disclose your details if required to the police, regulatory bodies or legal advisors. In exceptional circumstances where we are concerned about your safety/wellbeing or consider you to be a risk to yourself or others we may share limited information both internally and with relevant third parties (for example ambulance, police, NHS trusts etc.) to ensure appropriate support is available.

We will only ever share your data in other circumstances if we have your explicit and informed consent.

The SU undertakes an annual review of who has access to information that we hold to ensure that your information is only accessible by appropriately trained staff, volunteers and contractors.

Marketing & Communications Preferences

Membership Communications
As a member, we believe you have a legitimate interest in hearing from the SU about the products and services we offer, what we are doing to represent you and opportunities that might be of interest to you. Occasionally, we may include information from partner organisations, our own social enterprises or organisations who support us in these communications.

Direct Marketing

As a charity, we need to fundraise to provide the services we offer to our members. Where you have told us that we can, we send marketing material to our members. We do not sell or share personal details to third parties for the purposes of marketing.

Controlling what you want to hear about

We make it easy for you to tell us how you want us to communicate, in a way that suits you. Our forms have clear marketing preference questions and we include information on how to opt out when we send you marketing.

If you do not want to hear from us, let us know when you provide your data or contact us at dataprotection@thesu.org.uk.

Keeping your information up to date

Mostly, we use the record of members provided by the Universities to maintain accurate data about you. Nevertheless, if your contact details change, you may want to contact the SU direct at dataprotection@thesu.org.uk.

Understanding the detail of our data security measures

When we process your data, we will have assessed the lawful justification for doing so, the parameters in which the data is processed, the length of time the data is held, the secure storage of your data and undertaken impact assessments to ensure your rights are delivered.

The SU operates a Data Protection and Information Security Policy, which is supported by a practical handbook for our employees and volunteers. All employees and volunteers handling data are required to undertake general data protection training and third parties handling data are required to provide a contract that meets the requirements of the Information Commissioner's Office.

The SU does not store any sensitive payment card data on our systems during or following online transactions.

Your right to know what data we hold about you, make changes or ask us to stop using your data

You have a right to ask us to stop processing your personal data, and if it is not necessary for the purpose you provided it to us (e.g. processing your membership or registering you for an event) we will do so. If you have any concerns, contact us at dataprotection@thesu.org.uk.

You have a right to ask for a copy of the information we hold about you. If there are any discrepancies in the information we provide, please let us know and we will correct them.

If you want to access your information, you should complete a **Subject Access Request Form** with a description of the information you want to see and send that to us with the required proof of your identity to the Data Protection, The Students Union, Penryn Campus, Penryn, Cornwall TR10 9FE.

For further information see the **Information Commissioner's guidance**.

Changes to this notice

From time to time, we may change this Privacy Notice. We will also review this notice annually. If we make any significant changes in the way we treat your personal information we will make this clear on our website or by contacting you directly.

If you have any questions, comments or suggestions, please let us know by contacting dataprotection@thesu.org.uk

The Students' Union Advice Service Privacy Notice

Falmouth & Exeter Students' Union ('the SU') is a data controller and is committed to protecting your personal data and working in accordance with all relevant data protection legislation. Your data is collected so we can set up relevant and timely support, so you can make the most of your academic studies. This privacy notice explains how the SU's Advice Service ('the Advice Service') processes and uses the personal data we collect from current and prospective students.

What data do we hold?

The Advice Service may hold data relating to you from a number of sources. Some of the data we hold on students is data that you provided to your University[5], either before you commenced your studies or during your time as a student and which, in turn, the University has provided to us[6]. Other data is data that you provided to the Advice Service direct. This may include any forms you complete for us, documents including medical evidence/diagnosis of a disability, study needs assessment reports), appointment details, calls and emails.

Our records include:

- Personal Identifiers and biographical Information – for example your student ID number and your date of birth
- Contact details – for example your address, email address and telephone number
- Sensitive personal data -for example, information you have told us about your case
- Dates of meetings held with you
- Family details – for example details of other family members with whom you have given us consent to liaise

How do we use your data?

The Advice Service primarily uses your data to set up relevant and timely support, enabling you to focus on your academic studies and make the most of your time at university. Examples include:

- Offering you an appointment that is suitable to your needs and requirements
- Sending you information on how to set up support both within the Advice Service and externally if appropriate
- Advising and assisting you in relation to the issues that you have raised with the Advice Service.

These activities are essential to our service offering and all communications are intended to be respectful and sensitive to students seeking support from the Advice Service, or who may have been referred to our service by University staff or other third parties.

The Advice Service may communicate with you by telephone, text, email, post or other electronic means.

---

[5] i.e. University of Exeter or Falmouth University

[6] The SU has data sharing agreements with each of the University of Exeter and Falmouth University. To request a copy of that agreement, email the SU at dataprotection@thesu.org.uk

The Advice Service also collects routine statistical information about each contact made which is later anonymised and analysed for audit and evaluation purposes. This information may subsequently be summarised and interpreted in Advice Service and the SU reports. Care is taken to ensure no individually identifiable information is disclosed.

In exceptional circumstances where we are concerned about your safety/wellbeing or consider you to be a risk to yourself or others we may share limited information both internally and with relevant third parties (for example ambulance, police, NHS trusts etc.) to ensure appropriate support is available.

How will we share your data?

Other than with your written authority (or other than in **exceptional circumstances** as outlined below), the Advice Service will not disclose your personal data to third parties. You will be asked to sign a 'Consent to Liaise' form, on which you confirm whom we may or may not contact. In other instances, you may be asked to email us with the name of the person with whom you wish us to liaise.

How do we protect your data?

Any information disclosed to the Advice Service is stored within the Compass Online data system operated by FX Plus[7]. The databases are accessible to all Advice Service staff.

Any routine statistical information for service reports is anonymised before analysis.

In most instances, we will keep your data on our database for 7 years, following our last year of contact with you.

Your rights and preferences

If you ask the Advice Service to delete your data, we will consider this on a case-by-case basis. However, for compliance/legal reasons we will be unable to remove all records of the support you have received.

Other information

This Privacy Notice will be kept under review and will be formally reviewed on a yearly basis. Any changes will be updated on our website and communicated to you as appropriate. This Privacy Notice was last updated in May 2018.
You have the right to:

- Ask to see, correct or delete the data we hold about you
- Object to specific data uses, as described above
- Ask for the transfer of your data electronically to a third party

[7] FX Plus Limited is a company owned jointly by the University of Exeter and Falmouth University for the purpose of delivering shared services to their respective students

The SU's Chief Executive Officer (CEO) is responsible for monitoring compliance with relevant legislation in relation to personal data and can be contacted at dataprotection@thesu.org.uk. You can also contact the SU if you have any queries or concerns about the Advice Service's processing of your personal data. You have the right to lodge a complaint with the Information Commissioner's Office at www.ico.org.uk/concerns.

Further information

If you have any questions regarding this privacy notice please contact the SU on 01326 255861 or by emailing dataprotection@thesu.org.uk.

Staff Data Privacy Notice

Introduction

Falmouth & Exeter Students' Union ('the SU') is a data controller and is committed to protecting your personal data and working in accordance with all relevant data protection legislation.

This privacy notice explains how the SU processes and uses the personal data we collect from current and prospective employees.

This privacy notice relates to current and prospective employees who work for or have an expressed an interest in working for the SU in a role under which they have or would contract with the SU directly[8].

Where we collect information about you from

We collect information in the following ways:

When you apply for a role
When you apply for a role with the SU, you will complete an application form. This form will contain personal information about you. The SU has a duty to process this data for the purpose of considering you for that role. We will only share your application form with the interview panel. If your application is unsuccessful, we will keep your records for a maximum of 6 months, by which time they will be securely deleted from our servers.

When you become an employee
When you become an employee of the SU you form a contract with us which declares that we will process some personal and sensitive data to comply with our legal obligations and to fulfil our policies and procedures.

When a third party provides us with your data
Your information may be shared with us by independent organisations such as Her Majesty's Revenue and Customs or external references. These independent third parties will only do so when you have indicated that you have given consent or there is a legal obligation to share this data with us. You should check their Privacy Policy when you provide your information to understand fully how they will process your data.

What personal data we collect and how we use it

The type and quantity of information we collect and how we use it depends on why you are providing it.

[8] Therefore, it does not relate to those staff working for the SU under a contract with Falmouth University

Candidates

- If you are applying for one of our roles we will ask you to provide:
- Name
- Address
- Email Address
- Telephone Number
- Ethnic Origin
- Disability
- Employment and volunteering history
- Details of criminal convictions
- Details of training provided
- Relationship status with any the SU employees

If you are applying for a student staff role we will also ask you for the following details:

- Student Number
- Course of study
- Dates of study

We will use your data to:

- Communicate with you
- Provide anonymous equal opportunities monitoring
- Consider your application for the role

Third Party References

If you are a referee for an applicant, the applicant will provide the SU with the following information for the purposes of making contact to request a reference if the candidate is successful at application:

- Name
- Profession
- Address
- Telephone number
- Email address

Employees

When you commence employment with the SU we will ask you to provide:

- Name
- Address
- Email Address
- Telephone number
- Date of Birth
- National Insurance Number
- Photo (for university IT account)
- Bank Account Details
- Third Party Remuneration Sources

- Emergency contact details
- Evidence of the Right to Work

During your employment, the SU may collect the following data:

- Health records and physician details
- Performance records

We will use your data to:

- Administrative functions relating to your employment including the payment of salaries
- Managing sickness, health and workplace performance

How we keep your data safe and who has access

We undertake regular reviews of who has access to information that we hold to ensure that your information is only accessible by appropriately trained staff.
All our suppliers run their operations inside the European Economic Area (EEA). They are subject to same data protection laws as companies based in the UK. By submitting your personal information to us, your personal data will be stored or processing at a location inside the European Economic Area.

We disclose your information to key suppliers with whom we hold contracts to deliver services for the SU. These suppliers are named below:

Supplier:	Falmouth Exeter Plus
Purpose:	(1) For the creation of University associate accounts and ID badges (2) IT services that could be used for storage purposes. This includes but is not limited to Email, OneDrive, SharePoint.
Supplier:	Charities Aid Foundation Bank Limited
Purpose:	Payment Transfers
Supplier:	People's Pension
Purpose:	Pension service

In addition to these named parties, we may be required to disclose data containing limited personal information to auditors and financial advisors. Strict processing conditions shall be in place controlling what these parties can and cannot do with your personal data.

We may need to disclose your details if required to the police, regulatory bodies or legal advisors.
We will only ever share your data in other circumstances if we have your explicit and informed consent.

Keeping your information up to date

Employees are required to inform the SU's Finance and Administration Manager in the event of any changes to data or the discovery of any inaccuracies.

Understanding the detail of our data security measures

When we process your data, we will have already carefully assessed the lawful justification for doing so, the parameters in which the data is processed, the length of time the data is held for, the secure storage of your data and undertaken impact assessments to ensure your rights are delivered.

The SU operates a **Data Protection and Information Security Policy**, which is supported by a **handbook** for its staff.

All employees and volunteers handling data are required to undertake general data protection training and third parties handling data are required to provide a contract that meets the requirements of the Information Commissioner's Office.

Your right to know what data we hold about you, make changes or ask us to stop using your data

You have a right to ask us to stop processing your personal data, and if it is not necessary for the purpose you provided it to us for we will do so. If you have any concerns, contact us at dataprotection@thesu.org.uk

You have a right to ask for a copy of the information we hold about you. If there are any discrepancies in the information we provide, please let us know and we will correct them.

If you want to access your information, you should complete a **Subject Access Request Form** with a description of the information you want to see and send that to us with the required proof of your identity to Data Protection, The Students' Union, Penryn Campus, Penryn, Cornwall TR10 9FE.

For further information see the **Information Commissioner's guidance.**

Changes to this notice

From time to time, we may change this Privacy Notice. We will also review this notice annually. If we make any significant changes in the way we treat your personal information we will make this clear on our website or by contacting you directly.

If you have any questions, comments or suggestions, please let us know by contacting dataprotection@thesu.org.uk

Trustee Data Privacy Notice

Introduction

Falmouth & Exeter Students' Union ('the SU') is a data controller and is committed to protecting your personal data and working in accordance with all relevant data protection legislation.

This privacy notice explains how the SU processes and uses the personal data we collect from current and prospective trustees.

This privacy notice relates to current and prospective trustees who work with or have an expressed an interest in working with the SU in a role under which they have or would contract with the SU directly[9].

Where we collect information about you from

We collect information in the following ways:

When you apply for a position as trustee
When you apply for a trustee role with the SU, you will complete an application form. This form will contain personal information about you. The SU has a duty to process this data for the purpose of considering you for that role. We will only share your application form with the interview panel. If your application is unsuccessful, we will keep your records for a maximum of 6 months, by which time they will be securely deleted from our servers.

When you become a trustee
When you become an trustee of the SU you form a contract with us which declares that we will process some personal and sensitive data to comply with our legal obligations and to fulfil our policies and procedures.

When a third party provides us with your data
Independent third parties should only do so when you have indicated that you have given consent or there is a legal obligation to share this data with us. You should check their Privacy Policy when you provide your information to understand fully how they will process your data.

What personal data we collect and how we use it

The type and quantity of information we collect and how we use it depends on why you are providing it.

[9] Therefore, it does not relate to those staff working for the SU under a contract with Falmouth University

Candidates

If you are applying for one of our trustee roles we will ask you to provide:

- Name
- Address
- Email Address
- Telephone Number
- Ethnic Origin
- Disability
- Employment and volunteering history
- Details of criminal convictions
- Details of training provided
- Relationship status with any SU employees

If you are applying for a student trustee role we will also ask you for the following details:

- Student Number
- Course of study
- Dates of study

We will use your data to:

- Communicate with you
- Provide anonymous equal opportunities monitoring
- Consider your application for the role

Third Party References

If you are a referee for an applicant, the applicant will provide the SU with the following information for the purposes of making contact to request a reference if the candidate is successful at application:

- Name
- Profession
- Address
- Telephone number
- Email address

Trustees

When you commence a trustee role with the SU, we will ask you to provide:

- Name
- Address
- Email Address
- Telephone number
- Date of Birth
- Emergency contact details
- Bank details (for reimbursement of expenses)
- Driving licence or passport

We will use your data for administrative functions relating to your role as trustee

How we keep your data safe and who has access

We undertake regular reviews of who has access to information that we hold to ensure that your information is only accessible by appropriately trained staff.

All our suppliers run their operations inside the European Economic Area (EEA). They are subject to same data protection laws as companies based in the UK. By submitting your personal information to us, your personal data will be stored or processing at a location inside the European Economic Area.

We disclose your information to key suppliers with whom we hold contracts to deliver services for the SU. These suppliers are named below:

Supplier: Membership Services Limited ('MSL')
Purpose: For storage and access to trustee-related documentation

Supplier: Charities Aid Foundation Bank Limited
Purpose: Payment Transfers

In addition to these named parties, we may be required to disclose data containing limited personal information to auditors and financial advisors. Strict processing conditions shall be in place controlling what these parties can and cannot do with your personal data.

We may need to disclose your details if required to the police, regulatory bodies or legal advisors.
We will only ever share your data in other circumstances if we have your explicit and informed consent.

Keeping your information up to date

Trustees are required to inform the SU's Clerk to the Board of Trustees in the event of any changes to data or the discovery of any inaccuracies.

Understanding the detail of our data security measures

When we process your data, we will have already carefully assessed the lawful justification for doing so, the parameters in which the data is processed, the length of time the data is held for, the secure storage of your data and undertaken impact assessments to ensure your rights are delivered.

The SU operates a Data Protection and Information Security Policy, which is supported by a handbook for its staff.

All trustees handling data are required to undertake general data protection training and third parties handling data are required to provide a contract that meets the requirements of the Information Commissioner's Office.

Your right to know what data we hold about you, make changes or ask us to stop using your data

You have a right to ask us to stop processing your personal data, and if it is not necessary for the purpose you provided it to us for we will do so. If you have any concerns, contact us at dataprotection@thesu.org.uk

You have a right to ask for a copy of the information we hold about you. If there are any discrepancies in the information we provide, please let us know and we will correct them.

If you want to access your information, you should complete a **Subject Access Request Form** with a description of the information you want to see and send that to us with the required proof of your identity to the Data Protection, The Students' Union, Penryn Campus, Penryn, Cornwall TR10 9FE.

For further information see the **Information Commissioner's guidance.**

Changes to this notice

From time to time, we may change this Privacy Notice. We will also review this notice annually. If we make any significant changes in the way we treat your personal information we will make this clear on our Website or by contacting you directly.

If you have any questions, comments or suggestions, please let us know by contacting dataprotection@thesu.org.uk

Data Subject Request Form (Including Subject Access Request)

This form should be used to submit a data subject request under the provisions of the General Data Protection Regulation (GDPR).

Submitter Details

Name	
Address: (including email if applicable)	
Staff/Student Number: (or Other Unique Identifier)	
Relevant Dates: (Study/Employment etc.)	
Relevant Departments: (Study/Employment etc.)	
2 Forms of ID Provided: • 1 proof of identification i.e. Driver's Licence or Passport • 1 proof of address i.e. Recent Utility Bill (only required if request is not received via an @exeter.ac.uk or @falmouth.ac.uk account)	

Type of Request
Please select the type of request you are making:
(Select one only, if you wish to make multiple requests, please submit as a separate form, this will ensure appropriate processing of your request):

☐ *Consent withdrawal*
☐ *Access request*
☐ *Rectification of personal data*
☐ *Erasure of personal data*
☐ *Restriction of processing of personal data*
☐ *Personal data portability request*
☐ *Objection to processing of personal data*
☐ *Request regarding automated decision making and profiling*

Personal data involved

Request details

Provide as much description as possible (Course taken, staff/departments that may hold your personal data). Without further details provided, a reasonable search will be made based on the information provided.

Request reason/justification

Signature	
Date	

Submit this form by email to dataprotection@thesu.org.uk.uk or posted to:
Data Protection, Falmouth & Exeter Students' Union, Penryn Campus TR10 9FE

The data you provide in this form is collected so that you are able to exercise your lawful data subject rights under the GDPR. We will be required to share the data with the relevant departments/employees who may hold your personal data to enable us to respond to your request.

Once a request has been completed, the relevant data will be held for three years in line with ICO guidance. This is to ensure the by the Students' Union has carried out its requirements under the legislation.
For further information on how we process your personal data, please see:
http://www.thesu.org.uk/dataprotection/

Data subject access request procedure

Introduction

- Individuals have the right to access their personal data and supplementary information.
- The right of access allows individuals to be aware of and verify the lawfulness of the Falmouth & Exeter Students' Union's ('the SU') processing of their personal data.

What information is a person entitled to under the GDPR?	Confirmation that their data is being processed; Access to their personal data; and Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).
Charging a fee	The SU must provide a copy of the information **free of charge**. However, the SU can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The SU may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the SU can charge for all subsequent access requests. Fees must be based on the administrative cost of providing the information.
Timeframe	Information must be provided without delay and at the latest within one month of receipt. Where requests are complex or numerous, the SU may extend the period of compliance by a further two months. If this is the case, the SU must inform the individual within one month of the receipt of the request and explain why the extension is necessary.
Manifestly unfounded or excessive requests (including repetitive requests)	The SU may charge a reasonable fee taking into account the administrative costs of providing the information; or The SU may refuse to respond. Where the SU refuses to respond to a request, without undue delay and at the latest within one month, the SU must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.
How should the information be provided?	If possible, by remote access to a secure self-service system (best practice). If the request is made electronically, the SU should provide the information in a commonly used electronic format.
Requests for large amounts of personal data	Where the SU processes a large quantity of information about an individual, the GDPR permits us to ask the individual to specify the information the request relates to (Recital 63). The GDPR does not include an exemption for requests that relate to large amounts of data, but the SU may be able to consider whether the request is manifestly unfounded or excessive.

Data subject access request – processing form

The DPO should complete this form while dealing with the subject access request.

As such, this processing form is a 'working document'.

Step 1: Receipt of a request

Name of data subject	
Name and address of person/organisation (i.e. the agent) making request (if not the data subject)	
Evidence of agent's authority	Description:
Data subject's relationship with the SU	
University and student number (if appropriate)	Falmouth / Exeter (delete as appropriate) Student number:
Date on which request received	
Date on which request acknowledged – see Step 1 template email	
Target date for provision of response (being one month from date of receipt)	
Verification of the identity of the person making the request (see notes at the end of this document)	Documents provided: [enter] [enter]
Description of the information requested	

Step 2: Collating the information

Date on which details of request sent to the SU Teams – see Step 2 template email (below)			
Date by which the SU Teams should respond to Email 1			
Dates on which the SU Teams replied to Email 1	Student Opportunities		
	Advice Service		
	Central Services		
	Student Voice		
The SU Teams that hold information on the data subject	Student Opportunities	Y/N	
	Advice Service	Y/N	
	Central Services	Y/N	
	Student Voice	Y/N	
Provision of information by the SU Teams	**Team**	**Date by which Team expects to provide information***	**Date of receipt of information from Team**
	Student Opportunities		
	Advice Service		
	Central Services		
	Student Voice		
• **CHECK:** Does the date by which any Team expects to provide information compromise the date by which the data subject should receive their substantive response? • If so, update the data subject (or their agent).			
Date on which data subject updated (if relevant) – see template email below			
Reason for delay			
Revised date for provision of response			

Step 3: Reviewing the information

Information received from…	Does the information require redacting?	Date redaction completed (if appropriate)
Student Opportunities		
Advice Service		
Central Services		
Student Voice		

Step 4: Sending information to the data subject

Means by which information sent to data subject	
Date sent	

Step 1 template email

Dear [enter name]

Data subject access request

Your data subject access request has been passed to me.

I will be overseeing Falmouth & Exeter Students' Union's ('the SU') processing of your request.

We received the request on [enter date].

Under the provisions of the General Data Protection Regulation (GDPR), we are required to respond to your request within one month (i.e. by [enter date]).

We shall endeavour to respond before that date.

In circumstances where we are unlikely to be able to respond to you by [enter date], we will write to you to inform you and to explain why.

The scope of your data subject access request is:

"[enter]"

If you think we have misunderstood the scope of your request, please let me know as soon as possible. You can do this by emailing me at [enter email address].

Before responding to a data subject access request, the SU must check that the person making the request is who they say they are. With this in mind, please send me a copy of <u>one document from each of the two lists of documents</u> set out below.

List 1	List 2
Passport	Bank or building society statement issued in last 3 months
Biometric residence permit	Credit card statement issued in last 3 months
Current driving licence photocard (full or provisional)	Council tax statement issued in last 12 months
Birth certificate (issued within 12 months of birth)	Utility bill issued in last 3 months
Adoption certificate	

I look forward to hearing from you.

Yours sincerely

Step 2 template email 1

To Directors/Team Managers

The SU has received a data subject request from:

- [enter full name]
- [enter student number – if applicable]

The scope of the data subject's access request is:

- [Where possible, use the wording provided by the data subject in their request. In addition, if appropriate, provide additional guidance on the scope of the request]

Ordinarily, the SU has until [enter date} to provide the data subject with any relevant information.

Within two working days of receipt of this email, please complete the table below and email it to me:

Query	Reply
Does your Team hold any information about the data subject?	Yes/No
If yes, by what date do you expect to be able to provide me with copies of that information?	
If that date is after [enter date], please explain the reason for that delay. Because it may entitle us to extend the date by which we must provide the information to the data subject.	

Thank you…

Step 2 template email 2

Dear [enter name]

Data subject access request

I write further to my email dated [enter date].

As probably you are aware, ordinarily the Students' Union is required to respond to a data subject access request within one month.

In relation to your request, the relevant date is [enter date].

Unfortunately, we are not in a position to respond by that date. The reason for this is [enter reason].

Currently, we expect to be in a position to respond by [enter date].

The Students' Union apologises for the delay, but hopes that you understand the reasons for it.

Please let me know if you have any questions relating to the delay or your request generally.

Yours sincerely…

Step 4 template email

Dear [enter name]

The Students' Union's ('the SU') response to your data subject access request

Dear [enter name]

I write further to my email dated [enter date].

Please find attached, the SU's response to your request OR [how to access the relevant 'dropbox' or similar].

If you have any concerns about the way the SU has dealt with your request or any other questions relating to your request, please let me know.

You should be aware that if you do have any information rights concerns about the SU, ordinarily the Information Commissioner's Office (ICO) would expect you to raise that concern with the SU before raising it with the ICO.

Yours sincerely…

Data incidents and breaches: staff guidance

What to do if something goes wrong

Colleagues should understand the difference between an incident and a personal data breach:

An **incident** occurs where there is a risk of personal data being compromised. If handled quickly, an incident can often be contained before it becomes a breach.

A personal data **breach** is a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- The loss or theft of data in any format (e.g. papers taken from car, post intercepted, unauthorised download)
- Loss or theft or equipment used to store information (e.g. laptop, smartphone, USB stick)
- Compromised IT user account (e.g. spoofing, hacking, shared password)
- Blagging where information is obtained by deception (a person claims to be someone else)
- Accidental or unauthorised disclosure of information (e.g. email or letter to wrong recipient or incorrect system permissions/filter failure)
- Corruption or unauthorised modification of vital records
- Computer systems or equipment compromise (e.g. virus, malware, denial of service attack)
- Break-in at a location holding sensitive information or containing critical information processing equipment such as servers.

All incidents and breaches must be reported to:

- dataprotection@thesu.org.uk
- cc'ing the email to Richard Scrase (richard.scrase@thesu.org.uk)
- Karen Pardoe (k.pardoe@thesu.org.uk)

In Richard and Karen's absence, report your concern to:

- Sarah Davey (sarah.davey@thesu.org.uk)

When reporting an incident or breach, so far as possible you should:

- Describe what has happened
- State when the incident occurred (date and time)

- Identify those persons whose data or information rights may have been breached
- Attach any relevant documents or other evidence of the incident or breach
- Describe any action you have taken to contain the incident or breach

Time is of the essence

- By reporting an incident quickly, the SU can often contain it and avoid compromising the security of any personal data.
- The SU has a duty to report material data breaches to the Information Commissioner within 72 hours of the occurrence.
- Within the same timeframe, the SU may also need to notify the individual whose data protection rights may have been breached.

Remember…

…the Information Commissioner can fine the SU for data breaches and a failure to report a breach. The reporting of such fines may also cause the SU reputational damage.

Data Breach Management

The Students' Union ('the SU') is under a duty to document data incidents and breaches.

The person with responsibility for investigating and assessing any data breach should use this guide when completing a Data Breach Management Form.

1. Has there been a data breach?

A personal data **breach** is a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

2. Should the breach be reported to the Information Commissioner?

To establish the likelihood and severity of the resulting risk to the person's rights and freedoms, complete Section 3 of the Data Breach Form

Even if the SU decides it does not need to report the breach, we need to be able to justify this decision, so document it by completing Section 4 of the Data Breach Form.

3. Steps taken to contain the incident/breach

Section 5 of the form should be used to document all action taken by the SU to contain the incident or breach. The SU may need to demonstrate to the individual and the Information Commissioner or other relevant body, what action it has taken to contain an incident or breach. Such information also provides the SU with a useful body of information when considering any subsequent incidents or breaches.

Data Breach Management Form

The investigator should keep the incident/breach under review and add information, as appropriate. As such, the Data Breach Form is a 'working document'.

Following any change in the investigator's assessment of the incident/breach, the investigator should add information to this form. The investigator should not delete any earlier entries.

Section 1: Reporting of the incident/breach

Date and time incident reported NB: a material breach must be reported to the ICO within 72 hours of the breach	
Who reported the incident?	
How was the incident reported?	
Description of incident	
Date and time of incident	
If reportable to the ICO, date and time by which notice must be given	

Guidance note: complete Section 1 using the information provided by the person who reported the incident.

Section 2: Has there been a data breach?

Data breach?	**Reasons for reaching this conclusion**	**Date conclusion reached**
Yes / No		

Section 3: Risk assessment

What is the likelihood and the potential severity of the impact on the individual?

This assessment is designed to:

1. Help the SU take effective steps to contain and address the breach; and
2. Help the SU determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

Relevant factors	**Description / assessment**
The type of breach	
The nature, sensitivity and volume of personal data	
Ease of identification of individuals	
Severity of consequences for individuals	
Special characteristics of the individual	
The number of affected individuals	

Section 4: Notifying the ICO and/or individuals

Is the breach notifiable…	**Yes/No**	**Reasons for reaching this conclusion**	**Date conclusion reached**	**Date notification made**
…to the ICO?				
…to the individuals?				

A copy of any notifications should be stored with this form

Section 5: Steps taken to contain the incident/breach

Action taken to contain the incident	Date and time action taken	Anticipated impact of action	Actual outcome of action