

OXFORD SU: Student Advice Data Protection Policy

CONTENTS:

1. Statement of Purpose
2. Objective
3. General Principles
4. Data
5. Breaches of this Policy
6. Responsibility and Review

1: Statement of Purpose

Student Advice is a free, independent, and confidential information and advice service available to all matriculated Oxford University students.

Information is a key feature the Advice and its correct handling is vital to the delivery of the services and the integrity of the organisation.

In striking the right balance between collecting, storing, using and protecting information Student Advice must manage the impact and risks associated with maintaining the confidentiality, integrity and availability of information.

Within this context 'information' includes data and any form of communication recorded or transmitted in transcript or verbally, manually or electronically and the management principles extend to and include paper documents, computer files, electronic records or any other storage or processing medium.

This policy sets out the approach to be adopted to ensure that data is properly managed, protected against loss or compromise, is stored, removed and disposed of within legislative and best practice guidelines.

Student Advice is committed to -

- Complying with relevant legislation such as the Data Protection Act 1998, the Freedom of Information Act 2000 and the Computer Misuse Act 1990.
- Ensuring all staff are aware of their responsibility for the security of the data they are processing or accessing and their duty to comply with this policy and supporting procedures.

2: Objective

2:1 To provide Student Advice employees with a clear and concise policy and guidance that enables them to safeguard information and ensure that all necessary protective security measures are in place.

2:2 To inform Service Users steps taken to safeguard their data.

2:3 To ensure the Confidentiality, Integrity and Availability of SAS information in the support of operational and administrative requirements.

- Confidentiality:

(Ensuring that the information is not disclosed to unauthorised persons; specific details can be found in the Student Advice Confidentiality Policy)

- Integrity:
(Ensuring that the information is accurate and well maintained)
- Availability:
(Ensuring information is available when and where required)

2:4 To promote compliance with relevant legislation, regulation and to take account of recognised standards for good practice to manage the security of our information.

3: General Principles

3:1 Only those working for Student Advice and when necessary the Oxford SU CEO, should have access to data, both electronic and hard copy.

3:2 All data generated by the service must comply with the principles of the service Equal Opportunity Policy and Confidentiality Policy.

4: Data

4: 1 Data Collection: Only data relevant to the operational work of the service will be collected.

4:2 Data Use

Computer Use

- Password protected screen savers should be activated and employed when the authorised user is away from the computer.
- When sending emails that contain 'Confidential' information reasonable steps must be taken to ensure that the identity of the recipient is known and correct.
- It should be remembered that e-mails are subject to the Data Protection Act and may be legally admissible. As a result, care should be taken when using data not to expose the organization to legal liability or reputational damage.

Clear Desk Practice

- Best practice principles contain the concept of maintaining a clear desk – that is ensuring that all papers containing sensitive data are removed and securely stored when the office or desk is unattended.

4:3 Data Storage

Only data relevant to the operational work of the Service is stored for 7 years from the date of last contact.

Electronic Data

- When data is stored on computers, passwords must be protected
- Data must be saved to the secure server not the desktop

Hard Copy

- Hard copy data should be stored using service user initials, responsible caseworker initials and dated
- Hard copy data is subject to two levels of security. Data must be stored in locked filing cabinets in a room locked when not in use

4:4 Data Removal from the Student Advice office

Electronic Data

- Laptops containing confidential data must have an approved encryption device installed and activated. Users of devices (such as iPhones or iPad etc.) must use PIN or password activation where the facility is available.

Hard Copy

- Where hard copy 'confidential' information is physically removed for use outside the Student Advice office care should be taken regarding security.

4:5 Data Disposal

- Emails should be regularly reviewed to ensure those that are no longer required are securely deleted from the system.
- Hard copy data must be properly destroyed using approved confidential waste methods.
- Advice and guidance should be sought from IT Services on the disposal of ICT equipment to ensure that data is protected.

5: Breaches of this Policy

5:1 Breaches of this policy by staff will be regarded as misconduct and could lead to disciplinary proceedings.

5:2 Any member of the organization or service user concerned about a breach of this policy should follow guidance outlined in the Student Advice Complaints Procedure.

6: Responsibility and Review

6:1 The daily implementation of this Policy and supporting procedures will be the responsibility of all staff employed by the Organisation.

6:2 Operational oversight for the implementation of this Policy will lie with the Manager of Student Advice.

6:3 Ultimate responsibility for the implementation of this Policy will lie with the Chief Executive of Oxford SU.

6:4 This Policy will be reviewed annually or when required through Operational need. Review will be the responsibility of The Chief Executive of Oxford SU.

This Policy has been approved and authorized by

Name: J Hampton

Position President and Trustee

Date 28 February 2017

Date for Review February 2018

Related Policies

SA Code of Practice
SA Complaints Policy
SA Confidentiality Policy
SA Equality, Diversity and Non-Discrimination Policy
SA Exclusion Policy
SA Service Standards