

# University Student Services Confidentiality Policy

---

## 1. Introduction

Student Services believe students have the right to confidentiality to protect their interests and to ensure that relationships based on trust can be developed and maintained. Within a large institution a lot of personal data changes hands and it is important that every individual who handles personal data takes all reasonable steps to make sure it is treated carefully and only shared on a need to know basis. The University's standard response to enquiries about individuals is that information cannot be disclosed, even to family members, without the student's consent except in specific circumstances

There are different levels of confidentiality operating within different parts of the University. The Student Personal Data Code ([https://staff.shu.ac.uk/university\\_secretariat/disclosure\\_students.asp](https://staff.shu.ac.uk/university_secretariat/disclosure_students.asp)) provides information to students on how and why the University uses students' personal data. Certain professions have their own code of ethics which give clear guidance regarding confidentiality; these include counselling and related activities carried out by the Student Wellbeing Service and Childcare Services.

This confidentiality policy specifically covers the services provided by Faculty Student Services and the specialist Student Services provided centrally, listed below:

- Student Advice and Information
- Student Financial Support
- International Student Support
- Careers and Employment
- Student Wellbeing
- Disabled Student Support
- Sheffield Regional Assessment Centre

The policy makes users aware of the specific types of data held, the reasons for holding the data and the safeguards put in place to ensure the records are kept confidential. There are two key principles underpinning this policy:

- a. All staff are expected to treat personal disclosures sensitively and with respect so that a relationship based on trust can be developed and maintained. This will encourage students to come forward and seek help.
- b. Student consent should be sought whenever the need arises to share information. The reason for sharing information should be explained, with whom the information is to be shared agreed and the manner in which the information will be recorded made clear. Exceptions to this are covered in point 4 below.

## 2. Why do Student Services use personal data?

All Student Services obtain and retain data about service users. The purposes of this are:

- a. to enable us to administer and manage our services
- b. to enable users to access a particular service

- c. to enable any preparation to be undertaken in connection with an enquiry prior to an appointment
- d. to keep a record of user contact with a service to enable continuing work with users
- e. to provide advice and guidance based on accurate information
- f. to enable staff to communicate with users
- g. to enable us to monitor service usage anonymously
- h. to enable us to liaise with external agencies as appropriate to the service provision and with the users permission
- i. to enable us to provide anonymous data required by statutory bodies such as the Higher Education Funding Council for England (HEFCE)
- j. To enable us to provide data required by professional bodies such as Ofsted, RICS etc.

### 3. Which personal data does Student Services collect?

Our files include the categories of data below. Data is retrieved from the University's central Student Information (SI) system where possible. This avoids asking users to provide information already held by the university.

#### a) New clients

- |   |                             |
|---|-----------------------------|
| • Name and address                                    | • Local education authority |
| • Age/date of birth                                   | • Funding authority         |
| • Contact details                                     | • SI student ID number      |
| • Educational history including highest qualification | • Employment status         |
|   | • Course and stage details  |

#### b) Appointment data

- |                        |                 |
|------------------------|-----------------|
| • Appointment date     | • Meeting notes |
| • Referrals in and out | • Outcomes      |

#### c) Data collected for monitoring and reporting purposes

- |                  |                        |
|------------------|------------------------|
| • Ethnic origin* | • Student status       |
| • Gender         | • Nationality          |
| • Disability*    | • Socio-economic class |
| • Religion*      |                        |

\* These types of data are classified as sensitive personal data under the Data Protection Act 1998 and as such are subject to a greater level of control.

#### d) Additional data collected by Student Financial Support

- Details of students' and their partner's financial circumstances to enable their application for financial support to be assessed. This will include copies of relevant documentation for other agencies.

#### e) Additional data collected by Disabled Student Support and Student Wellbeing

- Medical evidence and impact of disability on learning
- Information relating to application for Disabled Student Allowances
- Students are asked if they wish to nominate a family member or friend with whom the service should share personal information relating to their disability and/or learning

needs

#### f) Additional data collected by Faculty Student Services

- Information relating to requests for extenuating circumstances or exceptional extension requests

## 4. Disclosure, Safeguards and Duty of Care

### a. How we handle personal data routinely used in providing our services

Users have the right to privacy of personal data. Access to all user data within the University whether on paper, computer files or other storage media, is strictly controlled. All users should be able to access services in confidence and therefore Student Services staff will not share any data with staff outside of their own Faculty or Directorate without the user's consent. All staff within Student Services regard personal data as confidential and will only access the data on a need to know basis as required in order to provide a professional service. Any breach of this confidentiality policy will be treated seriously and disciplinary action may be taken.

Within Student Services access to data is restricted on the basis of an individual member of staff's roles and responsibilities. Ordinarily staff will only be able to access the data within the team(s) they work in and only the data that is necessary for them to fulfil their role effectively. 'Teams' are those listed on page 1 of this policy.

Staff in management roles will have greater access as they are accountable for the control of data within their area of responsibility. Staff designated as Crisis Coordinators will have access to data which will allow them to make decisions quickly and efficiently in the event of a student crisis.

It can be to a student's advantage for staff to work collaboratively across Faculty or Directorate boundaries when considering a student's support needs. In these circumstances a user will be asked for their consent prior to releasing any personal data. Members of staff involved in a case will discuss with the student who else should be informed, what they should be told and who should pass on that information. The staff member will subsequently only make such disclosures as have been agreed with the student. We will routinely record where consent has been obtained prior to disclosure of information.

### b. How we handle sensitive personal data on disability and health

Data related to an individual's 'physical or mental health or condition' is classed as sensitive personal data. All Services require authorisation before releasing sensitive personal data outside of the Service Team. For example whilst disabled students are encouraged to disclose relevant information in order that the University can make reasonable adjustments, that data cannot be disclosed to other people without explicit consent (except in very particular circumstances listed in the policy). Students who receive an Assessment of Need or Study Needs Assessment and Learning Contract are asked to authorise release of their personal data. This includes:

- data provided in the Assessment Report being released to the relevant Funding body
- data provided in the Learning Contract being released to relevant University staff
- data about individuals may need to be disclosed in complex cases where a case conference is required to resolve a range of issues related to an individual (e.g fitness to practice panels)
- data required as supporting evidence for the submission of extenuating circumstances requests

Students who are using both Disabled Student Support and Student Wellbeing services are asked to consent to both services sharing personal information previously disclosed to either service. This only

happens when a formal referral between the two services has been made with the student's consent. A similar process exists between Student Wellbeing and Student Support within Faculties which is based on the student consenting to a referral being made.

c. How we respond to requests for personal data from the Students' Union

The Students' Union Advice Centre is independent of the University and students are encouraged to use the Centre for a range of queries. To enable Advisers to provide accurate advice it is often in the student's interest for the Adviser to have access to the University's student SI record. Students using the service will be asked to sign a form consenting to this information being released to the Advice Centre by the relevant Faculty.

d. Circumstances in which we may release personal data to third parties

There are certain circumstances where staff would disclose personal data without consent to third parties outside of the Service Team. In addition to those enquiries listed in the Student Personal Data Code these include the following:

*Personal data routinely released as part of the provision of the Service*

- disclosure to the University's Student Financial Support Panel for the purpose of assessing applications for emergency student funding
- disclosure of anonymised data to external agencies such as HEFCE, HESA or the Training Agency for statistical purposes. This may include releasing information to those services involved in providing the statistical return on behalf of another service (eg Student Financial Support on behalf of the Disabled Student Support team)
- disclosure of anonymised data where the University is required to participate in national surveys of students and graduates such as the Destinations of Leavers from Higher Education Survey (DHLE)
- disclosure to Student Finance England and the Student Loans Company in connection with grants, fees, loans, bursaries and scholarships
- disclosure to employers or other external agency when requesting references/verifications

*Personal data occasionally requested by third parties*

- disclosure to the Police and Immigration Service in order to comply with our statutory obligations. Where the police or immigration service are investigating a criminal offence in which a student may be involved, staff on reception points/help desks will follow University agreed procedures, managed by the Secretary and Registrar's Directorate.
- disclosure to callers in emergencies only, when in our judgement, it is in the student's interests to disclose information and where it is not possible to obtain the student's authority, the Head of Student Systems and Records or nominee would agree to provide the minimum necessary details to assist the enquirer, having first confirmed their credentials.

d. Circumstances in which we may release personal data without consent

Our standard response to enquiries about individuals is that information cannot be

disclosed without that individual's authority. This applies equally to enquiries from parents, guardians and other family members. There are however two circumstances where we may release personal data without consent:

*Serious harm to self or others*

Members of staff may disclose personal data without consent to people outside of their team where they consider it is in the 'vital interests' of the student. 'Vital interests' is defined by the Information Commissioner as matters of life or death. This will include where the student is perceived to be at risk; or where there is a serious risk of harm to others. The decision to release data without consent would normally be made by a senior manager (currently member of QESS Executive, Student Services Management team or Faculty Management team). This exemption is included within the Data Protection Act.

### *Critical Incidents*

The nature of personal support offered occasionally necessitates a group of staff working collaboratively across service teams and/or with university staff to respond in a timely way to a critical incident as part of the University's duty of care. In these circumstances efforts will be made to obtain consent from the user prior to the sharing of personal data as indicated above.

It is recognised however that there may be occasions where consent either cannot be given by the student or the member of staff would not reasonably be expected to obtain the consent. In circumstances where it is felt to be in the public interest, or interests of the individual, personal data may be disclosed without consent in order to provide appropriate counselling, advice or support services. In difficult situations we will keep accurate case records and will carry out risk assessments in line with the University's approach to duty of care.

### e. Safeguards

We recognise that users need to feel secure in using our services in a confidential manner. The following range of measures will be taken to ensure confidentiality:

- where appropriate users will be asked for their preferred method of communication
- all staff will be discreet when dealing with an enquiry and will ensure that confidential materials are not left visible to staff outside the service team.
- private interview space will be made available to users where possible and appropriate
- staff will ensure that when using private interview space no user data can be viewed or details overheard by other users using the service.

## **5. Responsibilities**

In line with the University's Student Personal Data Code we will

- set up and maintain user records promptly and accurately
- safeguard the privacy of individual users via a strict non-disclosure policy
- comply with all legal provisions in protecting all data on computers or in other formats from unauthorised access or use

In order to help us maintain meaningful records, users are asked to:

- provide accurate information when accessing our services
- tell us promptly about any changes affecting our records as appropriate

## **6. Case Recording and the Data Protection Act 1998**

All records are kept in accordance with the University's Policy on Records Management and the Records Retention Schedule. The Head of Service is responsible for document management for each service. All electronic data stored is password protected and rooms where manual data is stored are locked when empty or outside office hours.

Users may request access to their electronic or manual file by contacting the relevant Head of Service or Faculty Student Services Manager. Contact details for all our Heads of Service are available from Student Services reception or Faculty help desks. A user should expect to receive a response within 40 calendar days from their first enquiry, whether that enquiry is made verbally or in writing. This is in accordance with the Data Protection Act 1998. Should users wish to keep materials or to show them to other people, a copy can be made of the case file.

Claire Gandy, Head of Student Services, QESS

Faculty Student Services Managers:

Allison Briston (ACES), Sean Brown (D&S), Vanessa Coleman (H&WB), Carol Saunders (SBS)

June 2014

