Information Sharing Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Data - Chief Operating Officer - Compliance Committee
Is the Procedure for internal use only (Non-disclosable)?	Disclosable
Associated Policy Statements:	Our Colleagues - Chief People Officer Our Students - Chief Student Officer
Authorised Owner:	University Secretary and General Counsel
Authorised Co-ordinator:	Data Protection Officer
Effective date:	13/10/2023
Due date for full review:	3 years
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	New procedure	Compliance (data) Committee	12/10/2023

1. Purpose

The work of the University requires the sharing of information between staff, students, and (external) third parties. Seeking to maintain the open nature of the organisation, whilst also minimising the risk of loss, unauthorised disclosure, modification or removal of information maintained by the University; this procedure section aims to provide clarity on sharing information in a safe and secure manner.

Examples include, personal staff and student data, research data or other data and intellectual property covered by confidentiality agreements, commercial contracts, sensitive policy/committee documents, and examination papers prior to examinations.

2. Scope and Exceptions to the Procedure

- This procedure covers the sharing of information, and the mechanisms used to share such data. It covers all forms of information, whether held and shared in hard copy or electronic format. This procedure does not deal in detail with arrangements for bulk or pre agreed sharing of personal information between IT systems or organisations other than to explain their role in effective information governance.

- This procedure applies to all persons who process data on behalf of directly regards when using University IT networks and systems irrespective of whether the access is via an University owned and provided device or via any other device.

- Routine sharing of information happens regularly as part of day-to-day activities at the University. Examples include circulating or providing access to document workspaces or sending general emails. In these cases, information may ultimately be accessed both via University owned and non-University owned/maintained electronic devices. This policy is not limited to routine activities and includes data sharing processes such as:

    - research data shared by colleagues both internal and external to the university as part of a collaboration or agreement
    - Information shared with the police or other relevant bodies with legislative powers in response to a legitimate interest (i.e. under UK GDPR and the Data Protection Act).

- Information sharing may also happen as part of an automated process and therefore the process owner is responsible for ensuring the sharing complies with guidance within this procedure document.

- To support the effective information sharing appendix 1 provides guidance for colleagues to follow.

3. Definitions and Terminology

- **General Data Protection Regulation 2016/679** – is a law that sets guidelines for the collection and processing of personal information from individuals.

- **Data Protection Act 2018** – controls how your personal information is used by the University in support of GDPR 2016.

- **Personal data** - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in

particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- **Special Category Data** – relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life and sexual orientation

- **Users** – staff, students and others who are given access to University IT facilities, equipment, networks and systems.

4. Procedural Principles

4.1 Commitment

- Compliance with the requirements of this Procedure will ensure:
  - The University meets its statutory obligations in respect of legislation.
  - That exposure to non-ionising radiation is kept 'as low as reasonably practicable'.
  - Everyone is aware of their roles and responsibilities.
  - The safety and health of staff, students and visitors whilst working with lasers.
  - The safety and health of others (including contractors, members of the public) is not compromised by those persons working with lasers.
  - That staff, students and others who are authorised to work with lasers are appropriately informed, instructed, and where necessary trained and supervised.

4.2 Arrangements In order to meet the above objectives, the University will:

- Clearly define the organisational arrangements for achieving compliance (see roles and responsibilities section of this Procedure).
- Ensure resources are made available to achieve compliance.
- Periodically review and monitor the effectiveness and implementation of this procedure so that the compliance is maintained.
- Establish compulsory training requirements (including refresher training) for information sharing.
- Review sharing agreements arrangements periodically or whenever there are changes in relevant legislation, guidance, or University activities.

- Staff should be mindful to ensure their handling of information and applying of appropriate safeguards.

- Draft documents should normally be considered as confidential until they have been finalised or approved through the relevant line management or governance arrangements.

- It is the responsibility of those releasing the information to ensure that the recipient understands the confidentiality of the information and will abide by the provisions of this policy.

- **The Seven Rules to Effective Information Sharing**

  - Remember that the General Data Protection Regulation, Data Protection Act 2018 and the Human Rights Act are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
  - Be open and honest with the individual from the outset about why, what, how and with

whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

- Without disclosing the identity of the individual, where possible seek advice from other staff, or the information governance department, if you are in any doubt about sharing the information concerned.
- Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared. If there is no immediate danger to life, and you do not have specific consent to release the information, then it is good practice to seek advice from your information governance lead, particularly if the request has come from an external third party, including the police or other bodies with legislative powers.
- Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
- Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
- Keep a record of your decision in the relevant system or process and the reasons for it/whether it is to share information or not. If you decide to share, comment, then record what you have shared, with whom and for what purpose.

5. The General Data Protection Regulation (GDPR) and Data Protection Act 2018

- The General Data Protection Regulation and Data Protection Act 2018 (DPA) introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Staff must have due regard to the relevant data protection principles which allow them to share personal information.

- GDPR and DPA 2018 place greater significance on organisations being transparent and accountable in relation to the use of the data. All organisations handling personal data need to have comprehensive, in proportionate, arrangements for collecting, storing, and sharing information.

- GDPR and DPA 2018 do not prevent, or limit, the sharing of information for the purposes of keeping staff and students safe.

- To effectively share information:
  - All staff should be confident of the processing conditions, which allow them to store, and share the information that they need to carry out their role. Information which is relevant to the process will often be data which is considered special category personal data meaning it is sensitive and personal.
  - When staff need to share special category personal data they should be aware that the DPA 2018 includes safeguarding of children and individuals at risk as a condition that allows staff to share information without consent.
  - information can be shared legally without consent, if a staff member is unable to, or cannot be reasonably expected to gain consent from the individual, or if to gain consent could place the subject at risk.
  - Relevant personal information can be shared lawfully if it is to keep a person or individual at

risk, safe from neglect or physical, emotional or mental harm, or it is protecting their physical, mental, or emotional well-being.

- Sharing information is an intrinsic part of any staff member's role specially when working with students or vulnerable adults. The decisions about how much information to share, with whom and when, can have profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right support at the right time and prevents the need from becoming more acute or difficult to meet.

- Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of individuals. Every staff member must take responsibility for sharing the information they hold, and individuals cannot assume that someone else will pass on the information, which may be critical to keeping an individual safe.

- Necessary and Proportionate - When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and DPA 2018, and you should consider the impact of disclosing information on the subject and any third parties. Information must be proportionate to the need and level of risk.

  Relevant - Only information that is relevant to the purpose should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

- Adequate - Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

- Accurate - Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

- Timely - Information should be shared in a timely fashion to reduce of risks of missed opportunity to offer support and protection to the individual. Timeliness is a key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore put an individual at increased risk of harm. Staff should ensure that sufficient information is shared, as well as considering the urgency with which to share it.

- Secure - Wherever possible, information should be shared in an appropriate, secure way.

- Record - Information sharing decisions should be recorded, whether or not the decision is taken to share. Like the decision to share, reasons should be cited including what information has been shared and with whom, in line with the University procedures. If the decision is not to share, it is good practise to record the reasons for this decision and communicate them to the requestor in line with the University's retention schedules, the information should not be kept any longer than is necessary. In some rare circumstances this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

- Advice - Where there may be legal implications to the request it is good practice to discuss the response regarding the decision not to share with your information governance department prior to communicating with the requestor.

5.1 **Implementation: Communication Plan**

The key elements of this Procedure which require communication to all users on University policy pages.

- Relevant committees will also be notified, and information disseminated through line management.
- This procedure will be communicated through training to staff
- This procedure and relevant supporting documentation are also published on the University's Information Governance SurreyNet pages

5.2 **Implementation: Training Plan**

- Any required training will be offered out by the Information Governance Department as and when required in support of this procedure on the SurreyNet pages.

5.3 **Review**

- This Procedure will be reviewed every three years.

5.4 **Legislative Context and Higher Education Sector Guidance or Requirements**

- UK General Data Protection Regulation 2016
- Data Protection Act 2018
- Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019
- Human Rights Act 1998
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

5.5 **Sustainability**

- This procedure has no impact on carbon emissions or on energy consumption.

6 Stakeholder Engagement and Equality Impact Assessment

6.1 An Equality Impact Assessment was completed on 15/09/2023 and is held by the Authorised Co-ordinator.

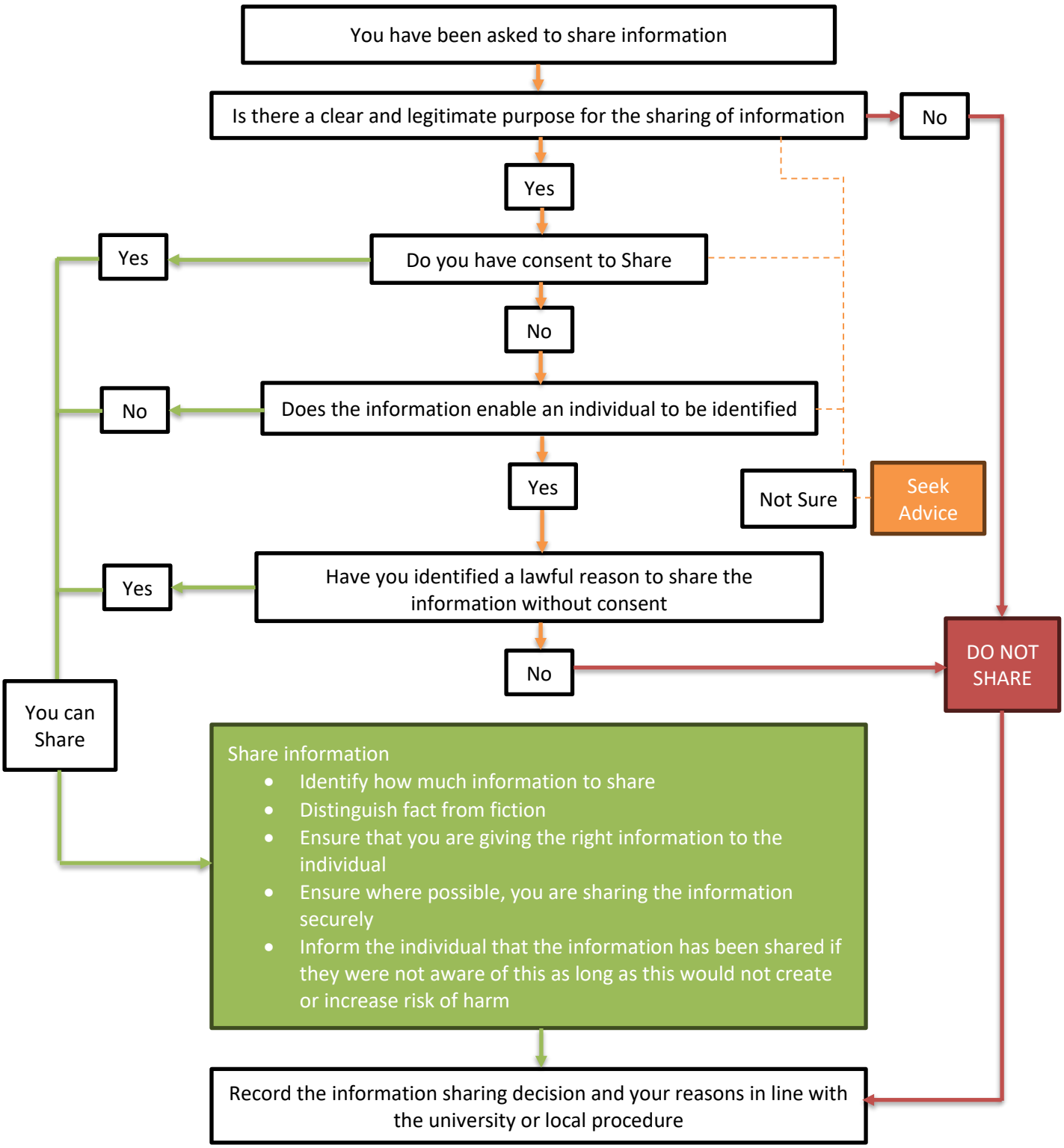
6.2 Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Request EB Approval (Y/N)**	**Date**	**Name of Contact**
Governance	Development and creation of this procedure	N	26/09/2023	Andrea Langley
H&S	Development and creation of this procedure			Matthew Purcell
Sustainability	Development and creation of this procedure			Martin Wiles
Chief People Officer – Our Colleagues	Development and creation of this procedure			Karen Raymer
Chief Student Officer – Our Students	Development and creation of this procedure			Kerry Mattews

School of VET Medicine	Development and creation of this procedure		21/09/2023	Kate English
Head of Campus Safety	Development and creation of this procedure			Mark Chatterton
Centre for Well Being	Development and creation of this procedure			Laura Smythson
OSCAR	Development and creation of this procedure			Glenn Moulton

Appendix 1

Should I Share -



If there are concerns that an individual is in need, or there is a immediate and real risk of causing harm to themselves or to others, then follow the relevant procedures without delay. Please ensure that the outcome of the discussion is recorded.

N.B. – Consent must be unambiguous, freely given and may be withdrawn at any time