Collegiate University Data and Information Sharing Protocol

A framework to guide the sharing of personal information across the collegiate University.

Contents

1. Introduction 3
2. Definitions and Interpretation 5
3. Legal Framework 6
4. Deciding Whether to Share Information 7
5. Governance and Review 7
6. Guiding Principles 8
6.1 Principle 1: Transparency about Information Sharing 8
6.2 Principle 2: Sharing Information for Clear and Legitimate Reasons 9
6.3 Principle 3: Sharing to Protect from Harm 10
6.4 Principle 4: Sharing to Prevent Potential Harm 11
6.5 Principle 5: Appropriate and Purpose-Focused Sharing 12
6.6 Principle 6: Respecting Confidentiality in Information Sharing 13

1. Introduction

1.1 This Protocol has been jointly developed by the University and the colleges to set out an agreed approach for individual colleges and the University when making decisions about the sharing of personal information relating to students and staff, including deciding whether to seek information or advice from others, both between individual colleges and between colleges and the University.

1.2 This Protocol has been developed following consultation across the collegiate University. It should be read alongside college and University policies, rules, and regulations, including the existing Data Sharing Agreements between each college and the University.

1.3 Nothing in this Protocol alters the status of each college and the University as separate legal entities and data controllers.

Purpose

1.4 This Protocol sets out a series of Guiding Principles which outline the agreed approach to the sharing of information between colleges, and between colleges and the University, as separate legal entities (both in terms of colleges sharing information with the University, and vice versa).

1.5 This Protocol is intended to operate as a coherent framework for decision-making. Its sections and Guiding Principles should be read together and applied collectively, recognising that decisions about information sharing will often involve balancing a range of relevant considerations in each context.

1.6 The purpose of this Protocol is to encourage a confident and purposeful approach to information sharing. Personal information must be shared responsibly and appropriately where this supports welfare, safety, disciplinary processes, or effective decision-making across the collegiate University.

1.7 Caution and uncertainty about when and how to share information, as well as reluctance or fear of doing the wrong thing, can lead to information not being shared where it may be lawful, appropriate, and important to do so. This Protocol is intended to facilitate a move away from unnecessary caution and support confident, responsible information sharing, recognising that data protection law provides a framework for good decision-making, rather than a reason to avoid the legitimate sharing of information.

1.8 Decisions about sharing information will sometimes involve uncertainty and questions of judgement. In some situations, people may feel that the safest course is not to share information; however, failing to share information can itself create risks. This Protocol recognises that there may be risks both in not sharing and in sharing information, and is intended to support individuals in making considered, defensible information sharing decisions.

1.9 Those involved in making decisions about information sharing should understand this Protocol as encouraging appropriate, lawful sharing. Colleagues should feel confident to share information when this supports welfare, safety, disciplinary processes, or effective decision-making, subject to the safeguards and considerations set out in this Protocol, and to record information sharing decisions appropriately where this is advisable or required.

Scope

1.10 This Protocol sets out Guiding Principles that college fellows and staff, and University staff, should follow when making decisions about the sharing of personal information between colleges, and between colleges and the University, in the contexts of:

a. student Support and Fitness to Study, Fitness to Practise, and Fitness to Teach;

b. student, fellow and staff health and welfare; and

c. disciplinary processes for students, fellows, and staff.

1.11 While the primary focus of this Protocol is the sharing of information between colleges, and between colleges and the University, it may also be applied in other contexts where personal information is shared. This may include sharing within colleges, within the University (where not covered by existing policies and guidance) and, where relevant, with external bodies such as the NHS, the police, and other statutory services.

1.12 This Protocol does not override or replace legal obligations or existing college or University policies, rules, or regulations. It is intended to guide their consistent and appropriate application in matters involving the sharing of personal information, and to set good practice standards for information sharing across the collegiate University.

2. Definitions and Interpretation

2.1 For the purposes of this Protocol:

- "**College**" means any of the Colleges, Permanent Private Halls, or Societies of the University of Oxford as defined in Statute V of the University of Oxford's Statutes.
- **"Fitness to Practise"** and **"Fitness to Teach"** processes consider whether a student or staff member is suitable to enter a regulated role, focusing on their conduct, professionalism, and any risks to others.
- "**Harm**" refers to physical injury, psychological or emotional distress, or risks to an individual's safety, wellbeing, or ability to engage effectively in their studies or work. Harm may affect the individual concerned or others.
- "**Personal information**" means personal data as defined in applicable UK data protection legislation. This includes personal data in all its oral, electronic, and paper forms, such as welfare, health, safeguarding, disciplinary and employment-related information relating to an identified individual.
- **"Privacy Notice"** is a formal document that informs individuals about how an organisation collects, uses, stores and protects their personal data.
- **"Risk**" refers to the possibility that harm may occur, taking into account both the likelihood of that harm and its potential seriousness.
- "**Safeguarding**" is defined as protecting a person's health, wellbeing, and human rights, and enabling them to live free from harm, abuse and neglect.
- "**Special category data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9(1) GDPR).
- "**Support and Fitness to Study**" is a process designed to support students if they are experiencing difficulties that affect their ability to continue studying and engaging with university life. Information can be found here.
- "**University**" means the Chancellor, Masters and Scholars of the University of Oxford.

3. Legal Framework

3.1 This Protocol operates within the framework of applicable data protection legislation, including the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

3.2 Personal information may only be shared where there is a lawful basis under Article 6 GDPR (see Guiding Principle 2), and, where relevant, an additional condition under Article 9 GDPR for special category data and/or an additional condition under Article 10 GDPR for criminal conviction data.

3.3 This Protocol does not alter those legal requirements but is intended to support their confident and appropriate application in practice.

Thresholds for sharing information

3.4 Information **must** be shared where sharing is necessary for compliance with a legal obligation or to meet an immediate safeguarding concern, for example where there is a risk of serious harm to a student, member of staff, or others, or where a safeguarding referral to external authorities is required.

3.5 Information **may** be shared where doing so supports welfare, safety, disciplinary processes, effective decision-making, or the prevention of harm, and where there is a lawful basis for doing so, for example sharing emerging concerns with relevant colleagues to enable early support or coordinated action.

3.6 Information **must not** be shared where there is no lawful basis for doing so, for example sharing personal information out of curiosity, convenience, or informal discussion where there is no clear purpose.

4. Deciding Whether to Share Information

4.1 The Guiding Principles set out in this Protocol should enable individuals to decide for themselves whether to share personal information, and with whom, and to feel confident when doing so.

4.2 Occasionally, there may be particularly complex, sensitive, or difficult situations in which a person may feel unable to make a decision without seeking further guidance.

4.3 Each college should identify an advisor, or a small number of advisors, and ensure that their identity and contact details are known within the college. The advisor should have appropriate seniority, experience, and access to information, and will act as a source of support and guidance for individuals in complex, sensitive, or difficult situations with whom information can be shared in confidence. The advisor should receive appropriate training.

4.4 The role of the advisor is to support decision-making in cases of complexity, sensitivity or difficulty. Individual decision-makers should have confidence in exercising their own judgment in other cases in accordance with this Protocol.

4.5 The advisor may seek further guidance from the statutory authorities and/or from appropriate teams within the collegiate University, provided this does not result in undue delay in decision-making.

4.6 The University has appropriate contact points who can provide support and guidance on decisions about whether to share personal information in complex, sensitive, or difficult situations, which should be communicated appropriately.

4.7 Where an individual decision-maker wishes to approach the University or the statutory authorities for guidance on information sharing, this should be done either by, or in co-ordination with, the advisor.

5. Governance and Review

5.1 This Protocol will be reviewed on an annual basis and updated in line with relevant legal and regulatory guidance.

5.2 Relevant teams will be briefed on the Protocol to support its implementation. Relevant existing training and guidance should also be updated, where appropriate, to reflect the Guiding Principles set out in this Protocol.

6. Guiding Principles

The following principles guide the approach to the sharing of personal information across the collegiate University. Each Guiding Principle is accompanied by a rationale and guidance on how it should be applied in practice.

6.1 Principle 1: Transparency about Information Sharing

When personal information is collected or first recorded, people should be told, in simple terms, about how, why, and with whom it may be shared as part of supporting welfare, safety, disciplinary processes or effective decision-making. In addition, people whose information is being shared should usually be informed of that sharing unless there is a clear reason not to do so, such as a risk of harm.

Rationale:

This principle encourages a thoughtful and balanced approach to transparency in relation to information sharing: be clear and honest about when and why information may be shared, without being unnecessarily technical, alarming, or restrictive.

Transparency operates at two levels. Firstly, people must be given clear information when their personal information is collected or first recorded about how it may be used and the types of circumstances in which it may be shared, and with whom. If such information has already been set out in existing documentation, such as Privacy Notices, data sharing tables, and related guidance, it is not necessary to do so again for the purposes of this Protocol.

Being open and transparent about how personal information may be shared is essential to maintaining trust and confidence. When people understand how their personal information might be used and with whom it might be shared, they are better able to engage with processes and services. At the same time, it is important to recognise that overly detailed descriptions of every possible sharing scenario can be confusing, discouraging, and overwhelming, and may unintentionally deter people from seeking support.

Secondly, people will usually expect to be told when and why their personal information is shared if the sharing takes place in a situation not covered by existing policies and procedures. There may, however, be situations in which telling someone about information sharing at a particular point in time may not be appropriate, for example where there is a risk of harm, safeguarding concerns, or a need to protect the integrity of a process.

Implications for practice:

Provide clear information for people, in simple terms, about how their personal information may be shared and why. Don't try to list every possible scenario; focus instead on the situations that are most likely to arise. When a person's information has been shared in a situation not covered by existing policies and procedures, ensure that they are told of this and explain why. However, also bear in mind that in some cases, it may not be appropriate to provide people with full details; consider what is appropriate in the circumstances. Where a decision is made to share personal information, ensure there is a clear record of what has been shared, with whom, and why.

6.2 Principle 2: Sharing Information for Clear and Legitimate Reasons

Personal information must be shared where there is a clear and legitimate reason for doing so, such as supporting welfare, safety, disciplinary processes or effective decision-making. Those sharing information should be able to explain the lawful basis or bases that they are relying on when doing so.

Rationale:

This principle encourages confidence in sharing information where there is a clear and legitimate reason to do so, so that it can be shared in a timely and effective way.

There is a need for greater understanding of the different reasons why information may be shared and of how they support responsible information sharing. Data protection law provides a range of bases for sharing information:

1. Consent
2. Contract
3. Legal Obligation
4. Vital Interests
5. Public Task
6. Legitimate Interests

The appropriate reason for sharing will depend on the nature of the information and the purpose of the sharing. Additional reasons are required for sharing special category (Article 9 GDPR) and criminal conviction (Article 10 GDPR) personal data.

In the contexts addressed by this Protocol, there will usually be a clear basis for sharing personal information, such as it involving a 'public task', there being 'legitimate interests', or it being a 'legal obligation' of a college or of the University.

In many cases, the reasons why information may be shared are explained in Privacy Notices, data sharing tables, and related documents published on college and University websites. These typically explain when and why information may be shared, for purposes such as academic administration, welfare, safeguarding, and disciplinary processes.

Implications for practice:

Be clear about why you are sharing information, and that the information you share is appropriate given the purpose of the sharing. Always remember to record your decision to share information where this is required by any formal process of which the sharing forms a part, or where decisions are complex, sensitive, or difficult.

Consent is sometimes relied upon as the default reason for sharing personal student information, particularly in welfare contexts. However, consent is not the only basis for sharing personal information, and over-reliance on the need for consent can sometimes delay or prevent appropriate information sharing.

6.3 Principle 3: Sharing to Protect from Harm

Personal information must be shared where there is a need to protect an individual or others from an imminent risk of harm.

Rationale:

This principle supports timely information sharing where there are clear or immediate concerns about safety or wellbeing.

In some situations, a clear concern, incident, or emerging risk requires immediate action. In these cases, sharing relevant information promptly can be critical to protecting students, staff, or others from harm and to enabling effective support or safeguarding. Failing to share information in such situations can inhibit effective safety planning and make it harder to respond effectively.

Implications for practice:

Where there is a clear concern or risk of imminent harm, consider what information needs to be shared, with whom, and for what purpose, in order to protect from harm and enable effective action. Where there is a clear need to act, data protection legislation does not prevent appropriate information sharing.

6.4 Principle 4: Sharing to Prevent Potential Harm

Personal information may need to be shared as a precaution at an early stage where emerging concerns suggest that doing so could help prevent harm from occurring or the escalation of a potentially harmful situation or incident.

Rationale:

This principle supports a preventive approach to information sharing where concerns are emerging but do not yet amount to an immediate risk of harm as outlined in Guiding Principle 3.

Not all concerns begin as crises. Low-level or emerging concerns may need early, coordinated support. Sharing limited and relevant information at this stage can prevent issues from becoming more serious and supports a preventive approach.

Implications for practice:

Where concerns are emerging, consider whether and to what extent sharing relevant information would support early intervention or coordination of services. Where sharing is appropriate, share information that is relevant and helpful at this stage, and review what is shared as the situation develops.

6.5 Principle 5: Appropriate and Purpose-Focused Sharing

Ensure that personal information shared is accurate, compatible with the original purpose of the sharing, and shared with only those who need to be aware of it because of their role or functions, but not more widely.

Rationale:

This principle supports thoughtful and balanced information sharing, where both the information shared, and the recipients of that information, are clearly linked to the purpose it serves and to the recipient's role.

Effective support for welfare, safety, disciplinary processes or effective decision-making often involves more than one person or body. Good information sharing means ensuring the right people have the information they need in order to perform their role or functions, while avoiding unnecessary or excessive disclosure. Overly restrictive approaches can block the effective coordination of services and prevent colleagues from carrying out their responsibilities properly.

Implications for practice:

When sharing information, consider what others need to know in order to carry out their responsibilities effectively. Share the information that is needed to allow appropriate action, but avoid sharing more detail than is required. Different recipients may need different levels of information, and the detail shared should reflect their role. If circumstances change, review what information has already been shared and consider whether further information ought to be provided, or whether any information that has been shared should no longer be relied upon.

Make sure that you share information clearly and securely. The potential significance of the material shared should be drawn to the recipient's attention and you should ensure that they understand what you have shared and why you have decided to share it with them.

6.6 Principle 6: Respecting Confidentiality in Information Sharing

Personal information must be shared and handled with care, used only for a purpose compatible with the reason it was shared for, and kept secure.

Rationale:

This principle emphasises that appropriate information sharing and confidentiality go hand in hand.

Confidentiality underpins trust. Respecting confidentiality does not prevent appropriate sharing; it ensures that shared information is used properly, kept secure, and not passed on without good reason.

Implications for practice:

If you receive personal information, be clear about why you have it and how it should be used. Use it only for the purpose for which it was shared, or for a compatible purpose, and do not pass it on without good reason. Keep it secure and only for as long as is needed, and in compliance with any applicable data retention policies. Review its use as circumstances change.