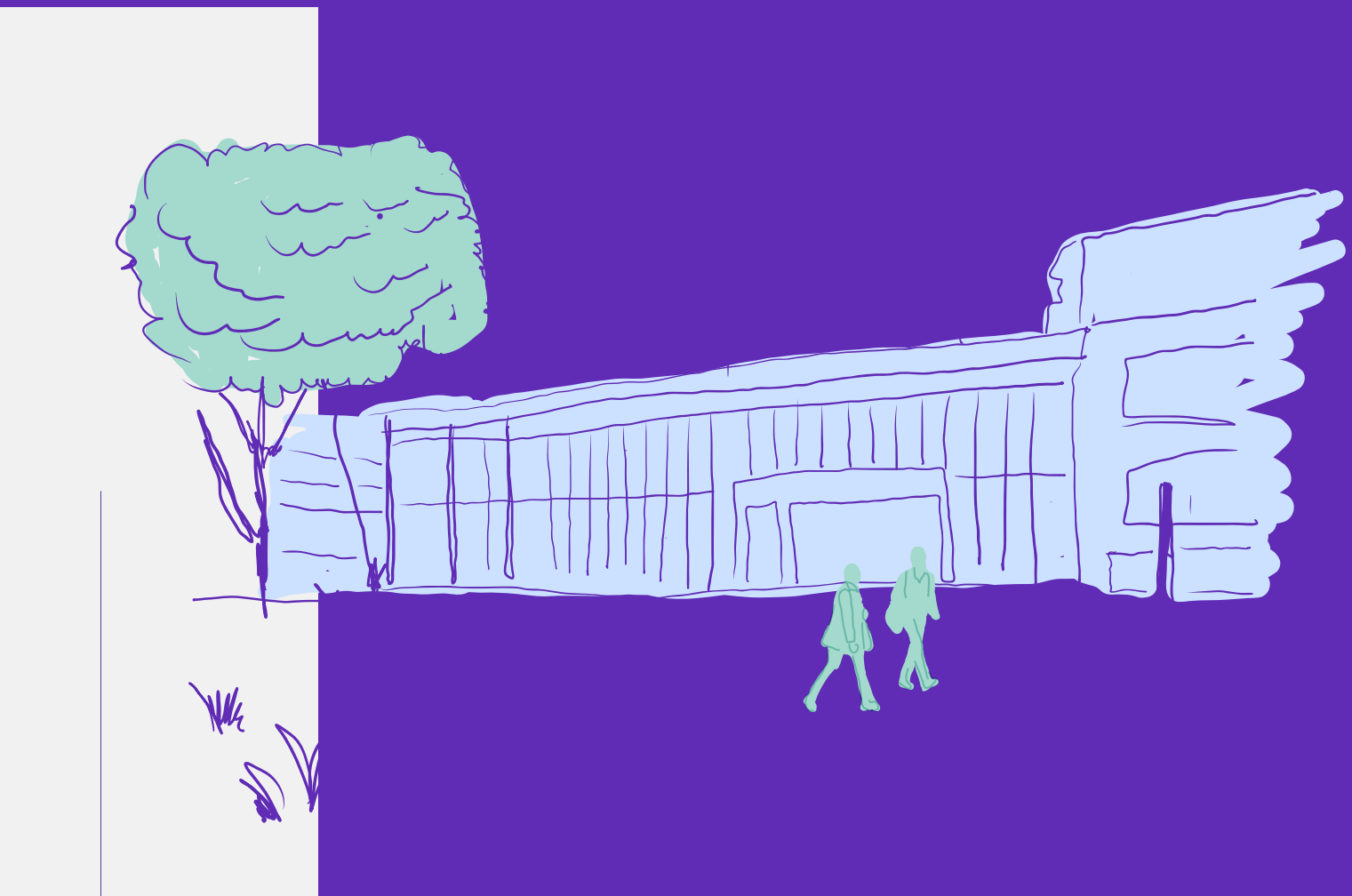
Universities UK

Coventry University

Changing the culture: sharing personal data in harassment cases

Practical guide for universities



Contents

1. Introduction

Structure

This Practical guide forms part of Universities UK (UUK) guidance on sharing personal data in harassment cases (**the guidance**).

The guidance contains UUK's practical recommendations for approaching decisions to share, or not share, personal data in relation to harassment cases. It particularly focuses on the sharing of information relating to outcomes and sanctions.

The Practical guide is structured as follows:

- **Section 2: Data Impact and Risk Assessment** tool to support universities when deciding whether to share personal data and for documenting such decisions.
- **Section 3:** Considerations for specific scenarios that have been highlighted as frequently asked questions throughout the preparation of the guidance.
- **Annexes 1–3:** Details around applying the data protection legislation underpinning this guidance.

This Practical guide should be read in conjunction with the accompanying **Strategic guide**, which sets out the underlying principles and themes of the guidance.

Please see Annexe 1 of the Strategic guide for a glossary of frequently used terms.

How to use this Practical guide

When deciding whether to share information universities will need to **balance the interests of, and risks to, both the reporting and responding parties. Each case must be considered on its specific facts.**

It is also important for universities **to manage the expectations of both reporting parties and responding parties** as to what information is likely to be shared, or not shared, about them or with them throughout the process, along with a practical explanation as to why.

This guidance cannot give definitive answers as to what a decision should be in a specific case. Whether or not to share personal data is ultimately a decision for the relevant university to take in accordance with its own internal governance processes and on the facts of the case in question. Who makes that decision within a university will depend on the internal governance processes.

There may be cases where it is **clearly appropriate to share or not to share personal data**. Examples include where there is a clear legal obligation or widely established practices such as in the context of employment law, or where there is a court order to release information. In these cases, a university may not need to carry out a full **Data Sharing Impact and Risk Assessment**.

Universities may decide to use the **Data Sharing Impact and Risk Assessment**:

- in complex cases where it is not clear if personal data should be shared
- to decide whether to share personal data in certain categories of situations; for example, in a harassment case, provided that each incident of sharing is still considered on its individual facts
- In any event, universities must satisfy themselves that they have considered both the data protection legislation and wider regulatory framework when deciding whether to share personal data and document such decisions in accordance with the accountability principle in Article 5 of the UK GDPR.

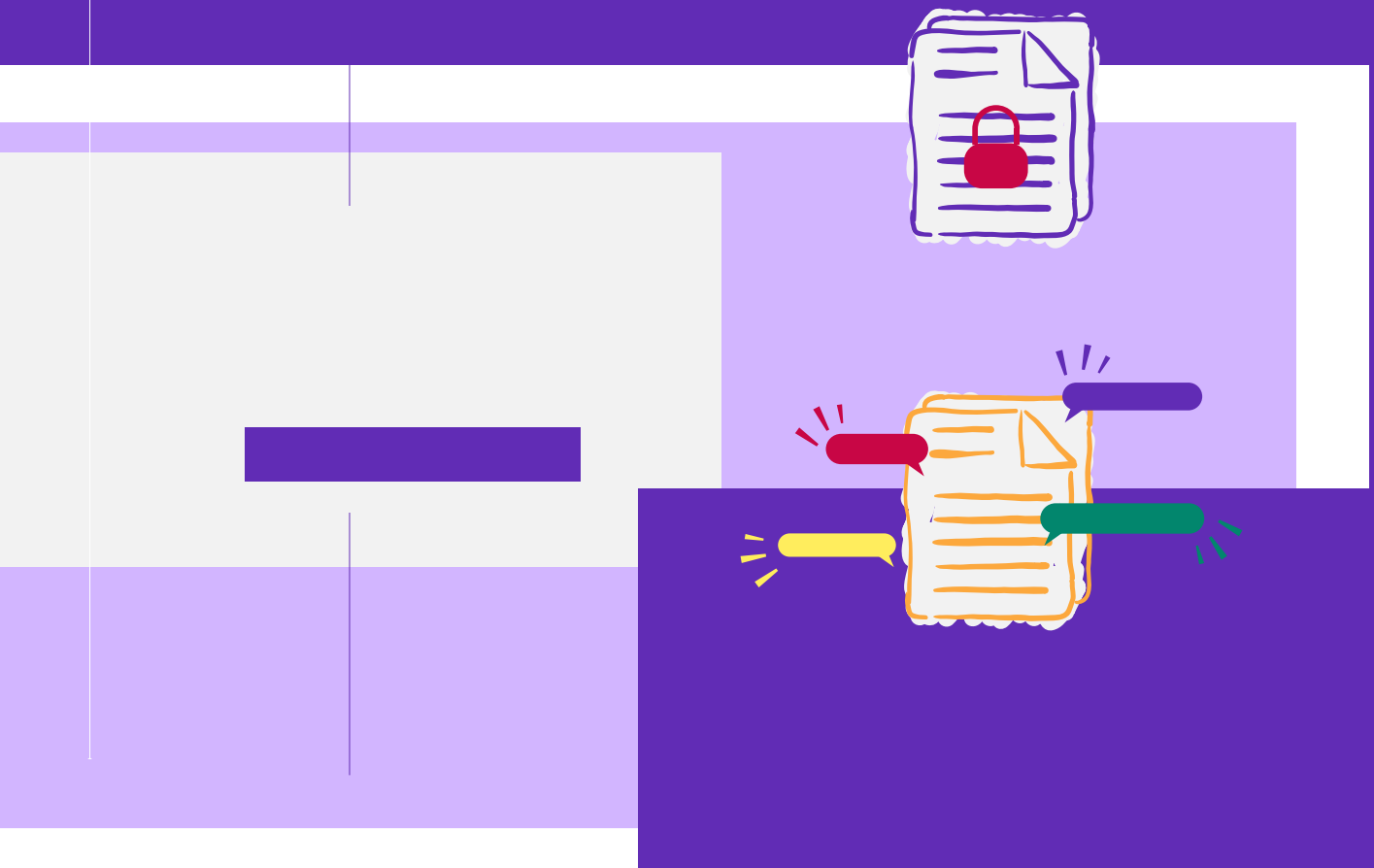
Guiding principles

The guidance follows several fundamental guiding principles, as set out in the Strategic guide and below for ease of reference. These underpin UUK's recommendations and should be considered when applying the guidance to real-life scenarios.

The data protection legislation is not a barrier to data sharing	Personal data can be shared where it is necessary, proportionate and justifiable to do so, where a lawful basis for the sharing can be established, and where the sharing is in line with the principles of the data protection legislation.
The data protection legislation should be considered in the context of the wider regulatory framework	The data protection legislation does not automatically take precedence over other legislation and is designed to work with and complement other legislation. The data protection legislation specifically allows for personal data to be shared in circumstances where this is necessary to comply with another legal obligation. Universities should also consider the wider regulatory framework when deciding whether to share personal data.

Rights granted under the data protection legislation apply equally to both the reporting party and the responding party	Universities should consider and balance the data protection rights, as well as fundamental equality and human rights, of both the reporting party and the responding party when deciding whether to share personal data in relation to harassment cases, and always in the context of the wider regulatory framework.
Decisions must be made on a case-by-case basis and on the facts of the case	Blanket policies to always share or always refuse to share personal data are unlikely to be lawful, and cases should be considered on their specific facts and risks to the individuals involved. This guidance provides a proposed framework for universities to follow when approaching decisions to share personal data in harassment cases. It provides a tool to guide universities through the decision-making process but cannot advise an institution as to what the decision should be.
Universities must decide how best to implement this guidance	This guidance provides a proposed process for universities to follow when making decisions to share personal data relating to harassment cases within the existing regulatory framework. It is for universities to determine how they implement this guidance in line with their own internal governance processes.
Transparency	To be effective in encouraging reporting parties to come forward, the outcome to a complaint should be as transparent as possible. Universities should maintain communication with all parties throughout the handling of harassment cases, sharing information where appropriate and lawful in accordance with the data protection legislation, and managing the expectations of all parties as to what information is likely or unlikely to be shared with them or about them, and why.

2. Data Sharing Impact and Risk Assessment



Overview: sharing personal data

For universities to share, collect or store personal data, universities must:

i. **establish at least one lawful basis for processing information under the data protection legislation**

- Information on the **six lawful bases** for processing and the relevance in processing personal data in harassment cases is set out in **Annexe 1**. This includes Article 6(1) of the GDPR, together with Article 9 where the personal data constitutes special category personal data.

ii. **ensure that it is necessary to share the personal data to meet the identified objective (or lawful basis), and that the personal data shared is limited to what is necessary**

- This requires universities to test whether the sharing is truly necessary, weighing up the interests of the reporting and responding party and any other individuals involved, the significance of the objective for sharing the information, and the contribution sharing that information would make to that objective.

iii. **ensure that the sharing of personal information can be processed in accordance with the data protection principles**

- The relevant principles and some suggested actions to demonstrate compliance with these are set out in **Annexe 2**.

iv. **comply with their obligations under the data protection legislation**

- A summary of some of the obligations most relevant to harassment cases are set out in **Annexe 3**.

Figure 1 below provides a **high-level summary** of the general underlying process to follow from the outset of any decision to share personal data in connection with a harassment case. This forms the foundation for the decision-making process set out in this guidance when deciding how and when to share personal data in connection with harassment cases.

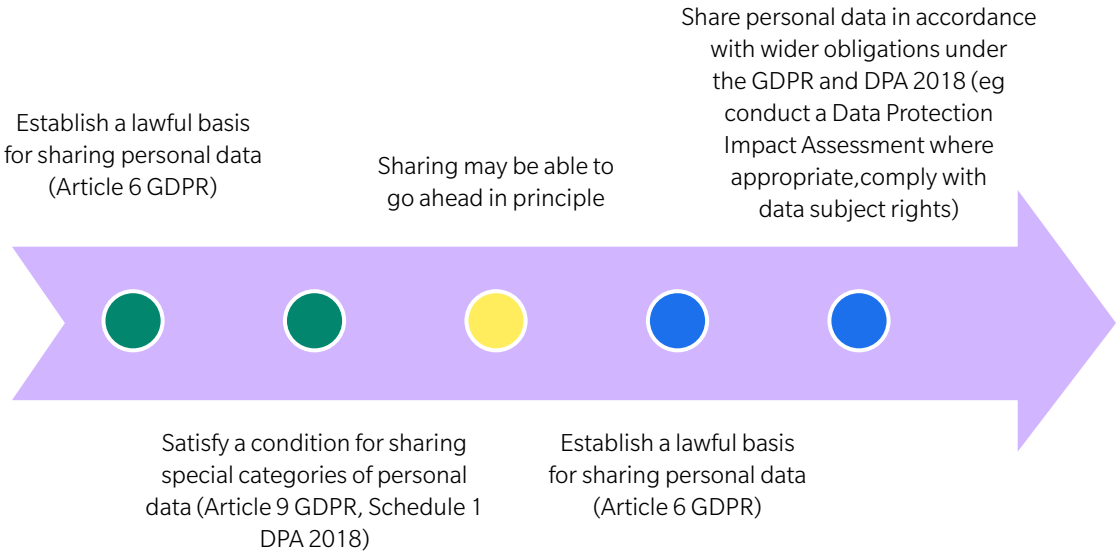


Figure 1. High-level summary of the general underlying process to follow from the outset of any decision to share personal data in connection with a harassment case.

Proposed Data Sharing Impact and Risk Assessment

The **Data Sharing Impact and Risk Assessment** is designed to help universities in testing whether the sharing of personal data is genuinely necessary and justified, taking into account the identified lawful basis for the sharing (see Annexe 1 for more information on lawful bases) and the relevant ICO data sharing guidance (Information Commissioner's Office, 2021).

This tool is designed to be used for complex cases where it is not clear if personal data should be shared, or where the sharing of personal data could be considered contentious or of a high risk to the parties involved.

The **Data Sharing Impact and Risk Assessment** includes example considerations when deciding if it is appropriate to share personal data. It can be used in relation to racial, sexual, or any other kind of harassment, bullying or misconduct cases relating to staff, students or other individuals within universities, whether in person, online or otherwise.

The tool focuses specifically on the first two stages of the data sharing process, highlighted in green in Figure 1.

In the limited circumstances where **special categories of personal data or criminal convictions data are to be shared**, universities will need to identify both an Article 6 and Article 9, 10 or Schedule 1 DPA 2018 lawful basis for sharing the personal data. (See Annexe 1 on how an institution might establish a lawful basis and which lawful bases are likely to be most relevant for harassment cases.)

Deciding whether to share

When deciding whether to share personal data in harassment cases, and to establish a lawful basis for such sharing, universities will need to follow the process outlined in **Figure 2**.

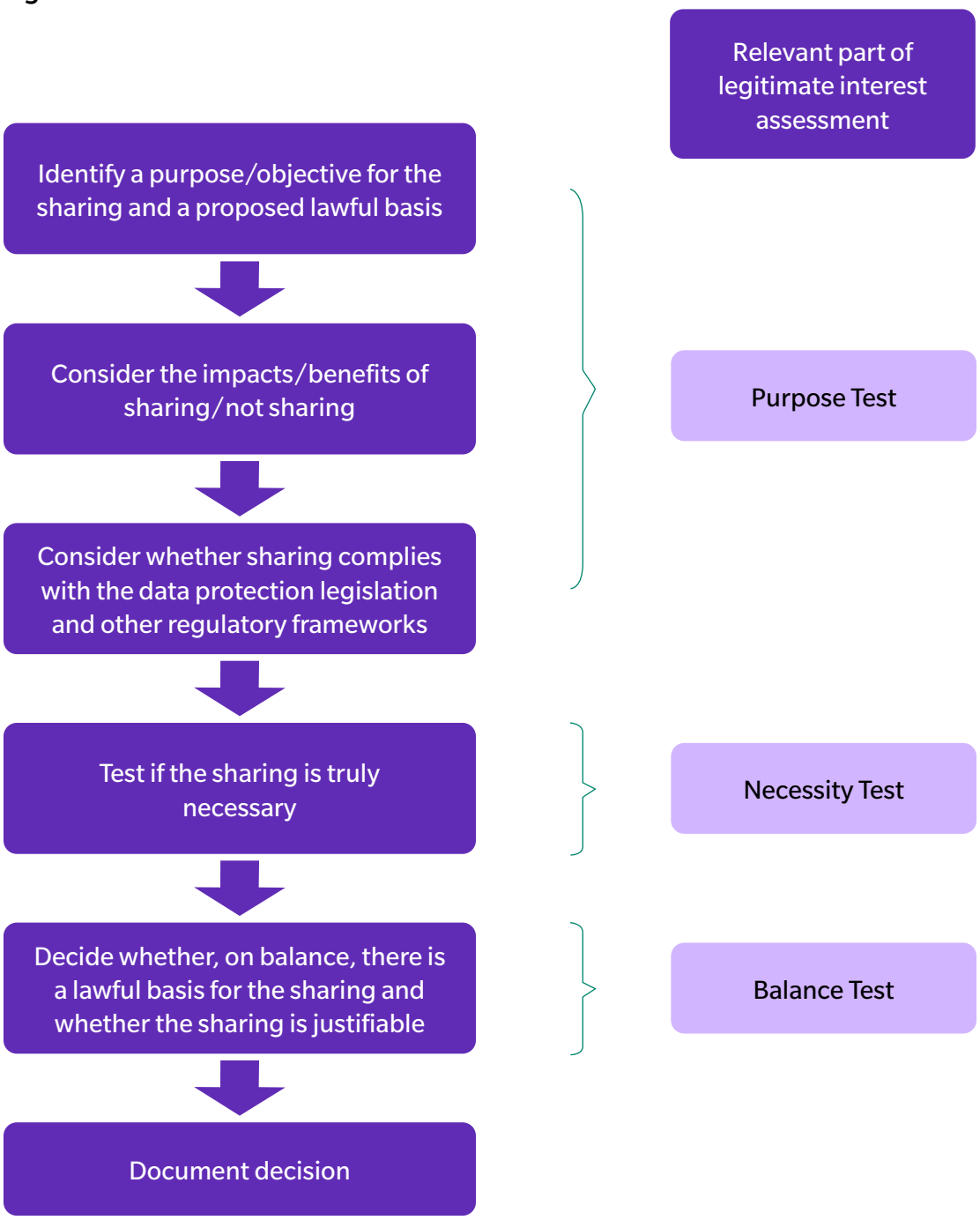


Figure 2. Process to follow when deciding whether to share personal data in harassment cases.

The Data Sharing Impact and Risk Assessment on the following page will guide universities through this process.

Data Sharing Impact and Risk Assessment

The Data Sharing Impact and Risk Assessment below combines the considerations recommended by the ICO when conducting a legitimate interests assessment (Information Commissioner's Office, 2018), and when sharing personal data as set out in the Data Sharing Code of Practice (Information Commissioner's Office, 2021). It includes specific considerations for universities when deciding whether to share the details of outcomes and/or sanctions with reporting parties, including considerations to help universities establish whether they have a lawful basis to share personal data, and whether such sharing is in accordance with the principles set out in the data protection legislation.

This expanded assessment is designed to assist universities when deciding whether to share personal data in harassment cases, as well as providing a template for documenting that decision.

Each point outlined below needs to be considered on balance. No single consideration takes precedent over others.

How to use this Data Sharing Impact and Risk Assessment

Universities should decide how best to use this Data Sharing Impact and Risk Assessment in accordance with their own internal governance processes. For example, it may be that universities use this template in its entirety only for complex cases, or they may decide to use it to assess whether to share personal data in certain categories of situations, notwithstanding that the specific facts of each case should still be considered each time personal data is shared.

While any decision to share personal data will need to be taken on a case-by-case basis, universities should ensure a consistent approach when handling any harassment case, in accordance with its own policies and procedures, wider guidance, the data protection legislation, and the wider regulatory framework.

It is important, both under the data protection legislation and wider regulatory framework, that individuals understand how a harassment case will be handled and how their personal data might be shared, as well as managing their expectations as to the information that could be shared with them or about them throughout the process.

Further special considerations for other specific scenarios related to harassment cases highlighted by UUK are set out in Section 3 below.

Part 1: Purpose test - identifying the objective of the sharing

What is the objective for sharing the personal data in connection with the particular harassment case?	
Proposed lawful basis	Insert proposed lawful basis under Article 6 of the UK GDPR. See Annexe 1 for further information.
Proposed additional lawful basis for sharing special categories of personal data	Insert proposed additional lawful basis under Articles 9 or 10 of the UK GDPR and/or Schedule 1 of the DPA 2018. See Annexe1 for further information.
Points to consider	**Suggested considerations for harassment cases**
a. **Why do you want to share the data? What is the objective of the sharing, and what is it meant to achieve?**	The objective(s) of the sharing should be clearly defined. For example, the objective of the sharing might be to reassure a reporting party that it is safe to remain on or return to campus. The Strategic guide outlines several reasons why it might be beneficial to share at least some information about outcomes and/or sanctions where possible, which could be used to help to identify the objective of the sharing.

b. **Can the same objective be achieved without sharing the data, or by anonymising it?**	Consider whether the objective can still be achieved without sharing personal data. If the objective could be achieved without sharing the personal data, the sharing is not strictly necessary and therefore the university will not be able to establish a lawful basis for the sharing. For example, it may not be necessary to give full details of a sanction imposed if the objective of reassuring a reporting party that it is safe to return to or remain on campus can be met by simply informing them that the responding party will not be on campus. On the other hand, it may be impossible to give effect to a sanction imposed if the reporting party does not have some awareness of what the sanction is. For example, where the sanction imposed on the responding party is to write a letter of apology to the reporting party, the reporting party would, by implication, need to be aware of the nature of the sanction in order to receive the letter of apology. Similarly, if the responding party has been told not to contact the reporting party or approach them on campus, the reporting party would need to be made aware of this to enable them to report to the university any incidents of non-compliance with such conditions by the responding party.

c. **Who requires access to the shared data to achieve the objective?**	Personal data, particular personal data relating to sensitive issues such as harassment cases and outcomes and sanctions relating to such cases, should only be shared on a 'need-to-know' basis. Universities should consider who needs to know about the outcome of a case or sanction imposed to achieve the identified objective. Consider that once personal data is shared with an individual in a personal capacity, a university will have little control as to who they might also share the personal data with, and the message given therefore needs to be managed carefully. For example, where sharing details about an outcome or indeed a sanction imposed, it is important to be clear that any finding is as a result of an internal process decided on the balance of probabilities, rather than a criminal process. We anticipate that universities will have appropriate support in place for reporting parties who also wish to pursue criminal proceedings.
d. **What benefit do you or the intended recipient of the personal data expect to receive from the sharing?**	The Strategic guide outlines several benefits of sharing information about outcomes and, where possible, sanctions with reporting parties, which could be used to identify the benefits of the sharing for the purposes of this section. For example, a potential benefit might be that the reporting party will be able to return to or remain on campus, or may be less likely to withdraw from their studies if they are given information about the outcome of a disciplinary process (for example, that the responding party will no longer be on campus or may only be on campus on certain defined days).

	If a reporting party is concerned about returning to or continuing with their studies, making them aware that a responding party has been asked not to approach them or has had their timetable changed so that they no longer will sit in the same sessions as the reporting party may make the reporting party feel more comfortable returning to their studies. Further benefits may be the reduction of psychological harm or impact on the mental health of the reporting party (for example, where they may find it upsetting to unexpectedly run into the responding party on campus), and to demonstrate to the reporting party that their complaint has been addressed appropriately. Universities must consider the potential benefits of the sharing from both the perspective of the reporting party and the responding party, which will then need to be balanced against the potential impact of the sharing (see further tests below). There must be a demonstrable line of causation between this potential benefit (for example, the reporting party is less likely to withdraw), the objective (for example, the reporting party feels safe to return to campus) and the sharing of the personal data.
e. **Are there any wider public benefits to the sharing of this information?**	For example, an institution may be able to demonstrate that the sharing of personal data may encourage an increase in reporting of harassment cases because reporting parties will have confidence that an institution will respond, and they will feel more satisfied with outcomes. In turn, this may lead to a safer environment in which to work, live and study. Again, there must be a demonstrable line of causation between this benefit, the objective and the sharing of the personal data.

f. **How important are the benefits that you have identified?**	For example, it may be that the potential benefits of the sharing identified above are important in the context of the university's compliance with the wider regulatory framework (ie sharing is considered to be an integral part of delivering an effective complaints regime, which in turn encourages complaints to be made) and general duty of care to staff/students, as well as an opportunity to promote the consequences of unacceptable behaviour more widely and thereby increase confidence in the complaints system.
g. **What would the impact be if you couldn't go ahead with the sharing?**	Consider the potential impact on both the reporting and responding parties if the sharing could not go ahead, particularly the impact of not sharing the information on the health and wellbeing, and personal and professional lives of both the reporting and responding parties. Not sharing information about outcomes and/or sanctions may mean that the reporting party feels unable to return to or remain on campus, or that their complaint hasn't been taken seriously, resulting in less confidence in the complaints regime. There may also be an impact on their health and wellbeing. Conversely, not sharing the information may avoid the potential negative impact that the sharing might have on the reporting party's personal/professional life, and health and wellbeing. The impact on both the reporting and responding parties will need to be carefully balanced, as set out in Part 3 of this assessment.

h. **Are you allowed or required to share the data?**	Consider whether there are any rules that might prohibit or require the sharing of personal data. For example, there may be some circumstances where the police need to know the outcome of an investigation or sanctions imposed as part of the management of their own investigation. (Note that where the police have obtained a court order for this information, universities have an established lawful basis for the sharing (Article 6(1)(c) UK GDPR, legal obligation and will not need to go through this assessment.)
i. **Are you complying with any specific data protection rules that apply to the sharing?**	Consider the wider obligations of the data protection legislation. Have individuals been made aware that their personal data might be shared and in what circumstances in relevant policies, notices and procedures, and/or by staff handling the complaint/ investigation (as appropriate)?
j. **Are you complying with other relevant laws?**	Universities must consider the wider regulatory framework to which they are subject. The data protection legislation does not automatically take precedence over other laws and makes provision for where another law requires the sharing of personal data. It should therefore be considered equally alongside the wider regulatory framework when deciding whether to share information. It is lawful under the data protection legislation to share personal data where necessary to comply with another legal obligation (Article 6(1)(c) of the UK GDPR; see Annexe 1 for further information), and a lawful basis for sharing can be established in these cases where there is a clear legal obligation. Conversely, it is not lawful under the data protection legislation to share personal data where such sharing is clearly prohibited by other laws. In preparing this guidance we have found that in most cases relating to the sharing of outcomes and/ or sanctions in harassment cases, there is often no clear legal obligation to share the information, or prohibition on such sharing.

In many cases, therefore, while the university may not be able to establish a lawful basis for the sharing under Article 6(1)(c) of the UK GDPR based on a clear legal obligation (see Annexe 1 for further information), it may still be able to establish another lawful basis for sharing at least some information about outcomes and/or where possible sanctions by completing this assessment. This section of the assessment therefore asks universities to consider whether their obligations under the wider regulatory framework support the sharing of information about outcomes and/or sanctions.

Universities should consider that the rights and protections afforded by the wider regulatory framework will apply to both the reporting and responding parties, and that there is a duty of care to both parties.

For example, Article 8 of the European Convention of Human Rights (ECHR) grants the right of respect for private and family life, except where interference with this right is justified, lawful, necessary and in other limited circumstances (where necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others). Depending on the facts of the specific case, a university may decide that sharing is prohibited by Article 8 to protect the responding party's right of respect for private and family life, or that it is justified in sharing the information with the reporting party (eg where necessary to fulfil its duty of care obligations to the reporting party). As the data protection legislation is derived from ECHR Article 8, the considerations set out in this assessment will aid universities in establishing whether interference with this right is justified, lawful and necessary in the circumstances.

k. Are you complying with industry guidelines or codes of practice?	Various industry guidelines or codes of practice contain information about when it may or may not be appropriate to share personal data. For example, OIA guidance (Office of the Independent Adjudicator, 2016), and equivalent guidance from the Scottish Public Services Ombudsman (SPSO) and Northern Ireland Public Services Ombudsman (NIPSO), requires that the outcome of the reporting party's complaint is shared with the reporting party, notwithstanding that the complaint may have led to a separate disciplinary process and a separate outcome/ sanction related to such disciplinary process. If a university is required by statute to comply with guidelines or codes of practice, and such guidelines or codes of practice clearly obliged the sharing of personal data to take place, the university will be able to establish a lawful basis for sharing under Article 6(1)(c) of the UK GDPR (see Annexe 1). However, if a university is not required by statute to comply with guidelines or codes of practice, or if guidelines or codes of practice do not contain clear requirements to share, the guidelines or codes of practice should still be considered here in deciding whether to share information on outcomes and/or sanctions. In complying with any guidance, universities should consider how much information should be shared for these specific purposes in the context of the wider regulatory framework, including the data protection legislation and other considerations set out in this Data Sharing Impact and Risk Assessment.

I. Is it right to share data in this way?	Consider whether, having looked at all relevant and specific circumstances of the particular case, it is right from an ethical perspective to share the personal data. Each case should be considered on its merits and the specific facts of the case, including the university's duty of care to the individuals involved and any specific health or wellbeing concerns of the reporting party, responding party and anyone else involved. For example, it may not be appropriate to share full details of the outcome of a disciplinary process or sanction imposed with a reporting party if the responding party has shared something deeply personal in the wider context of the proceedings that is inappropriate to share, or which is irrelevant to the reporting party's complaint, but omitting this information would create a misleading impression of the outcome. On the other hand, it may be ethically right to share at least some information about an outcome or sanction where the reporting party's health and wellbeing have been significantly affected by the incident, and the sharing of some information about the outcome or sanction would help them to feel safe on campus and continue with their studies/employment. As always, universities must balance the interests of both the reporting and responding parties.

m. Are there any other ethical issues with the sharing?	Consider the ethical arguments both for and against the sharing. This will include considering if the sharing is proportionate and fair in the circumstances, if it is right and justified to share the data, whether a responsible institution would share the data, and whether clear and strong safeguards are in place to protect the individuals involved. Consider any imbalance of power between the university and the individuals involved, and the need for universities to act responsibly towards those individuals and society more widely. Consider the impact that sharing may have on the rights and freedoms of the individuals involved, both from a data protection perspective, but also from a wider equality and human rights perspective. The rights of all individuals involved will need to be carefully balanced. For example, it may not be ethical considering the facts of the case to share full details of the outcome or sanctions imposed with the reporting party when considering the significant and damaging impact this might have on the responding party's personal life, health and wellbeing, and professional reputation. On the other hand, it may be ethical to share some information with the reporting party if to do so would help ensure their safety, health and wellbeing, and ability to engage in their studies, as well as encouraging zero-tolerance of harassment culture. This will need to be considered on balance and in consideration of the other sections of this assessment. Consider that any sanction imposed following an internal disciplinary process regarding breaches of policy and/or misconduct is made on the balance of probabilities, and that this is distinct from the criminal justice system where the execution of criminal penalties falls outside of the scope of the data protection legislation (see Article 2(2)(d) UK GDPR). As such, any information shared would need to be accompanied by careful messaging to explain how the decision was reached, considering the potential impact on the responding party if this was misconstrued.

n. When and how should the data be shared?	Consider how best to share and communicate the information in light of the circumstances and individuals involved (eg individuals may require reasonable adjustments or need further support when they receive the information). For example, if a university decides that it is appropriate in the circumstances to tell a reporting party that a responding party will/will no longer be on campus, consider that the reporting party may require additional support to continue their studies/ employment.
o. How can we check that the sharing is achieving its objectives?	Once the information has been shared with an individual in their personal capacity it will be impossible to retract the information if the sharing has not achieved its objectives. As such, care and caution must be exercised when deciding whether it is necessary and appropriate on balance to share personal data in relation to such cases, and the messaging around the sharing of information should be managed. It may be useful for universities to assess whether or not the identified objective has been achieved through the sharing of personal data, or a decision not to share personal data, to inform future decisions as to whether or not to share personal data, provided that all cases are dealt with on a case-by-case basis on their specific facts.
Comments: Detail any relevant information about how the university has taken into account the above considerations and outline the legitimate interest/objective of the sharing.	
DPO comments (if appropriate): If appropriate, liaise with the DPO to further consider the purpose and objective of the sharing.	

Part 2: Necessity Test

Is the sharing necessary for the identified purpose/objective?	
Points to consider	Suggested considerations for harassment cases
a. What information do you need to share?	Consider what information genuinely needs to be shared to achieve the objective. For example, if the objective of the sharing is to ensure that the reporting party feels safe to return to or remain on campus, depending on the facts, it may only be necessary to share with them that the responding party will no longer be on campus. In some cases, for a disciplinary sanction to be effective it may be necessary to share some details of the sanction with the reporting party. For example, if a responding party has been prohibited from being within a certain proximity of the responding party, it may be necessary for the reporting party to know about this so that they can alert the university of any breaches of this sanction, to prevent further harassment and to support the safety of the reporting party. Similarly, it may be necessary to share some details of a disciplinary sanction with the reporting party to give effect to that sanction; for example, where the responding party has been asked to write a letter of apology to the reporting party, clearly the reporting party will be made aware of the sanction through receiving such a letter. However, in many cases it may not be necessary to share full details of the sanction imposed on the responding party with the reporting party, and where sharing details of the outcome instead will be sufficient. For example, it may be sufficient to tell the reporting party that their complaint was upheld and that the responding party is no longer on campus for the reporting party to feel safe to return to or remain on campus and that their complaint has been addressed. The need to share the information must be genuine and demonstrable

	It may also not be necessary to share specific details of a sanction with a reporting party where a university has clear sanctioning guidelines outlining the categories of sanctions which may be imposed. Therefore, letting a reporting party know what the outcome of a case is may be sufficient for the reporting party to understand that the likely sanction to be imposed will fall into a particular band of sanctions depending on severity, without them needing to know the specific sanction imposed.
b. Is the sharing actually necessary to achieve the purpose/objective?	Universities should demonstrate a causal link between the objective and the sharing of the personal data, ie that the information needs to be shared to achieve the purpose/objective. This should be more than tenuous and must demonstrate a genuine need to share.
c. What would happen if the personal data were not shared?	It is helpful to assess the impact of not sharing the personal data to test whether the sharing is truly necessary. For example, universities may be able to demonstrate, on the specific facts, that it would be harmful to the reporting party's mental health not to share the information (for example, where they are concerned about seeing the responding party) and telling the reporting party that the responding party will not be on campus will avoid this. Conversely, the responding party's mental health, wellbeing, and personal and professional life will also be impacted by any sharing of information, and this must also be considered in the context of the circumstances of the case. The interests of both responding and reporting party need to be balanced, and any sharing of information would need to be limited to what it strictly necessary to avoid unnecessary harm to either party and to meet the specific objective of the sharing, as further explored in this assessment.

d. Can you achieve the same objective by sharing less personal data?	Only the minimum required personal data to achieve the objective should be shared. For example, if the objective is to ensure that the reporting party feels safe to return to or remain on campus and this can be achieved by telling them that the responding party is no longer on campus and will not be returning, in some circumstances it may not, in consideration of all of the factors set out in this assessment, be appropriate or lawful to share further details of the disciplinary outcome or sanction (eg the specifics around whether a responding party has been dismissed or in fact resigned before the sanction could be imposed).
e. Is the sharing proportionate to the purpose/objective?	Consider whether the sharing is proportionate to the objective on the specific facts of the case, in light of all of the possible risks, impacts and benefits. Universities should consider the inherent sensitivity of any information relating to harassment cases when deciding whether sharing is truly necessary. In considering this, universities should consider both the impact on the reporting party if information about outcomes and/or sanctions is not shared with them, balanced against the impact on the responding party of disclosing such information to the reporting party or anyone else.
Comments: Detail how the university has taken into account the above considerations and why the sharing is necessary.	
DPO Comments (if appropriate): If appropriate, liaise with the DPO to further consider the genuine necessity of the sharing.	

Part 3: Balancing Test

On balance, is the data sharing:

- appropriate, considering the impact on individuals' interest, rights and freedoms, and whether these override the university's legitimate interest (where lawful basis is legitimate interest)?[1]
- proportionate, considering the objective of the sharing and all circumstances of the case (where other lawful basis is relied upon)?

Nature of the Personal Data	
Points to consider	**Suggested considerations for harassment cases**
a. Is it special category data or criminal offence data?	Extra care should be taken when sharing special categories of personal data or criminal convictions data, and an additional condition for processing must be established (see Annexe 2). There are specific rules and protections around the sharing of criminal conviction data, notwithstanding that this may be in the public domain (eg where reported in the press), considering its severity and the significant impact that a criminal conviction may have on an individual's life, including their ability to work and to access education. Consider that sharing the outcome of disciplinary proceedings, or indeed the sharing of a sanction imposed, may have the same significant impact on a responding party as if they had been given a criminal conviction, without being afforded the same level of protection. The impact on the responding party of sharing information must be balanced against the impact on the reporting party, and any information shared must be accompanied by appropriate messaging to make clear that an outcome or sanction is not the same as a criminal finding.

1 Note that in many cases the university is will be acting in its capacity as a public body and will therefore be unable to rely on legitimate interests as a lawful basis. However, legitimate interests may be the appropriate lawful basis in relation to processing of staff personal data where the university is acting in its capacity as an employer. Please see Annexe 2 for further information.

b. Is it information that people are likely to consider particularly 'private'?	Information relating to harassment cases, be that the personal data of the reporting party, responding party, witnesses or otherwise, is inherently private by nature. The information is likely to have significant relevance to the personal life, studies and/or professional life of the individuals involved and must be handled with care. Consider that some information about the outcome of, or all information in respect of the sanction imposed in, a disciplinary process is inherently private to the responding party, and the release of this information could significantly impact their ability to work and/or access education, as well as their personal and family life. As such, caution must be applied to any decision to release information relating to the outcome of a disciplinary process considering its private nature and the potentially significant impact of sharing too much information, and messaging around any information shared must be carefully managed.
c. Are you sharing children's data or data relating to other vulnerable people?	Universities should consider their specific duties when sharing personal data relating to children (eg students who are under 18) or vulnerable people, and extra care should be taken to ensure that the sharing is necessary, proportionate and lawful on balance.
d. Is the data about people in their personal or professional capacity?	Consider that the information shared is likely to affect all individuals involved both personally and professionally, depending on the facts, and may have long lasting impact on either of these areas. Universities will need to consider whether it is proportionate and justifiable to share information considering the nature of the personal data.
Comments: Detail how the university has taken into account the above considerations and why the sharing is necessary.	
DPO Comments (if appropriate): If appropriate, liaise with the DPO to further consider the genuine necessity of the sharing.	

Reasonable expectations	
Points to consider	**Suggested considerations for harassment cases**
a. Do you have an existing relationship with the individual?	In cases involving staff and students, universities will have a pre-existing relationship and therefore more easy access to make individuals aware of how their personal data might be shared. Where information about another individual who is not a staff member/ student is to be shared (for example, where a member of the public comes forwards as a witness in connection with a harassment case) consider that this individual may not be aware of how their information might be shared, and they will need to be kept informed as to what will happen to their personal data.
b What's the nature of the relationship and how have you used data in the past?	Consider whether in the specific circumstances of the case, the individuals involved might reasonably expect their personal data to be shared based on the nature of the university's relationship with them and based on how other previous cases have been handled.
c. Did you collect the data directly from the individual? What did you tell them at the time?	Universities will need to be transparent as to when and how personal data might be lawfully shared, and update privacy notices accordingly. Further, universities must ensure that expectations of all relevant individuals are managed throughout any complaint, grievance or disciplinary processes by keeping in touch regularly. This includes managing the expectations of the reporting party and responding party both in what information about them will be shared with the other party, and what information will not be shared.

d. If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?	Consider whether it is appropriate to share personal data where such has been obtained from a third party. Was the information given to that third party, or given to the university by that third party, given in confidence? Would the data subject in question expect their personal data to be shared by the university? Consider the sensitivity of the information and the importance for accuracy (see Annexe 2 [add link]) when sharing any information in connection with harassment cases, and the need for the university to investigate any information appropriately and in accordance with its processes before sharing this.
e. How long ago did you collect the data?	Ensure that the information remains correct and consider whether the data subjects involved would expect their personal data to be shared if a period of time has passed since they gave this information.
f. Is your intended purpose and method widely understood?	Universities will need to ensure that privacy notices are clear and that they explain that, in certain circumstances, information (including outcomes and sanctions) may be shared where appropriate with other individuals, including reporting parties and responding parties, in connection with disciplinary and/or complaints processes. Ensure that staff involved in dealing with harassment cases understand when personal data might be shared to answer any queries from the individuals involved.
g. Are you intending to do anything new or innovative?	If there has historically been a blanket policy in relation to sharing of personal data in harassment cases (ie either to never share information or to always share information about outcomes and/or sanctions), it is important to raise awareness as to how this policy might have changed; for example, through updating privacy notices and explaining how and when personal data might be shared to the individuals involved in specific cases.

h. **Do you have any evidence about expectations, eg from focus groups or other forms of consultation?**	Universities should consider whether there is any evidence of what the reasonable expectations of staff and students might be, and consider this when deciding whether to share information, and more generally when raising awareness as to how data might be shared.
i. **Are there any other factors in the particular circumstances that mean individuals would or would not expect the sharing?**	Consider the specific circumstances of the sharing. For example, an individual may have specifically requested that some personal data is not shared (eg if they have provided some private details), or may have agreed that information is not shared as part of a settlement agreement. Notwithstanding the wider legal considerations around the sharing of such data, it may be more difficult to demonstrate that, on balance, the sharing should go ahead if the individual has received some assurance of confidentiality.
Comments: Detail how the university has taken into account the above considerations and why the sharing is necessary.	
DPO Comments (if appropriate): If appropriate, liaise with the DPO to further consider the genuine necessity of the sharing.	

Likely impact	
Points to consider	**Suggested considerations for harassment cases**
a. **What are the possible impacts?**	Consider all the impacts, both positive and negative, outlined in Parts 1, 2 and 3 of this Data Sharing Impact and Risk Assessment, and any further impact that sharing, or not sharing, may have on the individuals involved. The impact of sharing personal data about an outcome or, in limited circumstances, a sanction may have a positive impact on the reporting party. For example, this may have a positive impact on their health and wellbeing, and their feelings of safety when on campus. Sharing may also demonstrate that the complaint has been taken seriously, encouraging further reporting of harassment and other misconduct, and a culture of zero tolerance. Conversely, the impact of sharing information about an outcome or, particularly, a sanction may have a detrimental impact on the responding party. For example, this may have a negative impact on their personal and professional life, as well as their health and wellbeing. Universities must consider that a duty of care is owed to both the reporting party and responding party, and that the data protection legislation and wider regulatory framework applies equally to both parties.

b. **Will individuals lose control over the use of their personal data?**	In any case where information is shared with an individual in their personal capacity, the university is likely to effectively lose control of that information and the information could be shared more widely. This must be considered in the context of the inherent sensitivity of information relating to harassment cases. Any information shared should be limited to what is necessary and proportionate in connection with the objective of the sharing, and any messaging given when sharing any information must be carefully managed. Once shared, individuals share information more widely amongst colleagues, friends, across institutions and even in the press, and there will be little that universities can do to prevent this. Consider if, on balance, it is still appropriate and justifiable to share the personal data, notwithstanding that control over such personal data is likely to be lost, and consider whether any mitigations would be effective (eg asking the reporting party to keep the information confidential).

c. What is the likely severity of any potential impact? What risks does the data sharing pose to the individuals involved? What can be done to mitigate those risks?

Due to the inherently private and sensitive nature of any harassment cases, the potential impact of sharing on the individuals involved could be severe and must be considered on balance when deciding whether to share. For example, sharing information about the outcome of disciplinary proceedings, and in particular any sanction imposed, could have serious personal and professional consequences for the responding party, particularly if the outcome could be misinterpreted as a finding of criminal liability. Conversely, not sharing any information could have a detrimental impact on the reporting party who may feel that their report has not been properly considered by the university, discouraging future reports. To mitigate these risks, it might be possible to share limited information about the outcome of the disciplinary process to achieve the objective of the sharing, without revealing the full sanction imposed. Again, any such message must make clear that this is a finding of an internal process, not a criminal process, and does not carry any criminal finding, sanction or liability.

When weighing up any impacts risks, universities should consider the following:

Risk/Impact	Mitigating steps	Residual risk
What is the possible risk or impact of sharing the personal data?	What are the steps that can be taken to mitigate these risks/the impact?	Does the risk or impact remain, either in whole or part, after mitigating steps have been taken? If so, is it still appropriate, in consideration of all of the facts, to share the personal data?

d. Are some people likely to object to the sharing or find it intrusive?	Simply objecting to the sharing does not automatically mean that it cannot go ahead. However, universities will need to consider whether there are likely to be any objections when deciding, on balance, if it is necessary and proportionate to proceed with the sharing.
e. Would you be happy to explain the sharing to individuals?	If a university would feel unable to explain to the relevant individual, whether they are the reporting party or the responding party, why a decision to share personal data is justified, this would suggest that the sharing is not appropriate when considering all factors.
f. Can you adopt any safeguards to minimise the impact?	Considering the potentially significant impact of the sharing outlined above, consider if there is any scope for mitigating this impact. For example, is it possible to share less information while still achieving the same objective, or to mitigate the impact by managing messaging and expectations?
g. Are the individuals able to opt out of the sharing?	Consider that the responding party is unlikely to be able to opt out of the sharing of personal information about an outcome or sanction of their disciplinary process: if this option were given, almost all responding parties would opt out of sharing information. As such, it is important to ensure that the reasons that the university has established for sharing, or not sharing, through the assessment above are strong and justifiable, and demonstrably necessary to meet the identified objective.
Comments: Detail how the university has taken into account the above considerations and why the sharing is necessary and proportionate on balance.	
DPO Comments (if appropriate): If appropriate, liaise with the DPO to further consider necessity and proportionality of the sharing.	

Decision whether or not to share personal data	
Lawful basis relied upon to share personal data	Insert proposed lawful basis under Article 6 of the UK GDPR, eg performance of a contract, legal obligation, vital interests, public task (specify function or power), legitimate interest
Lawful basis relied upon to share special categories of personal data	Insert proposed additional lawful basis under Articles 9 or 10 of the UK GDPR and/or Schedule 1 of the DPA 2018
Is it appropriate and lawful to share the personal data?	YES / NO
Comments to justify decision:	
Data Sharing Impact and Risk Assessment completed by:	
Date	

3. Specific scenarios

This section outlines additional specific data sharing scenarios identified by UUK that may frequently arise in relation to harassment cases. It also highlights key considerations when using the tool in Section 2.

Specific scenarios

As above, all cases will need to be considered on their facts and on a case-by-case basis. The considerations below are provided by way of example, and there may be other considerations to take into account, depending on the specific case.

a. During and after the disciplinary process	
Sharing information with a reporting party during an investigation so that they can reply to evidence put forward by the responding party	In the interests of ensuring a fair and thorough investigation, it may be appropriate to verify facts with the reporting party in the context of the responding party's response to the original allegations. However, this will need to be considered in the context of the data protection legislation, as well as the wider regulatory framework and sector/industry guidance to which universities are subject. In any event, information should be limited to that which is necessary (for example, to test and verify the evidence), particularly as the investigation may be considering other issues in addition to the allegation raised by the reporting party.

Sharing information with the responding party about the reporting party	Under the principle of natural justice, and in accordance with the wider regulatory framework, guidance and codes of conduct, it will almost always be necessary to share comprehensive details of the allegations made with the responding party so that they are able to fully respond to the allegations made against them. In many cases, it will be unlawful not to share this information and to then seek to impose sanctions (such as dismissal or expulsion) on the responding party. Consider the potential impact of not sharing the information with the responding party on the reporting party and other staff/students. This will have a detrimental effect, as it will most likely be impossible to deal with the inappropriate behaviour and impose appropriate sanctions if the university is unable to run a proper investigation and disciplinary process due to full details of the allegations not being shared. Notwithstanding the above, universities will need to consider the potential impact of the sharing on the reporting party in light of the sensitivity of the information to be shared and safeguards that could be put in place to protect them. The responding party does not need to be made aware of personal information relating to the reporting party that is not connected to the allegations. For example, there may be some information that the responding party does not need to be made aware of, such as the reporting party's past unrelated experiences of abuse, suicide attempts, or health and wellbeing. As ever, the sharing of any information should be limited to that which is necessary for the objective (ie investigating the allegation, giving the responding party the opportunity to fully respond to the allegations in accordance with principles of natural justice, and taking appropriate action).

Sharing information about disciplinary proceedings with witnesses or other third parties	The sharing of any personal data should be on a need-to-know basis. Consider that it may be necessary on balance to share some information with a witness about whether the responding party is coming back on campus; for example, if they are particularly concerned about retribution or victimisation. It is unlikely to be appropriate to share information about disciplinary proceedings with third parties, as there is unlikely to be a justifiable reason for doing so, depending on the facts of the case. However, there may be some limited circumstances where such sharing is appropriate, for example: • A university may need to notify the police about something that has come to light during an investigation, particularly if there is an ongoing investigation or if there is a serious risk of harm. • It may be necessary for universities to share information with the OIA/SPSO/NIPSO in relation to the escalation of complaints. • It may be necessary for universities to disclose information in the context of employment tribunal proceedings, or to other relevant bodies in relation to fitness to practice. It is important to note that a lawful basis for sharing such personal data must still be established and the data protection legislation and wider regulatory framework still complied with, even for notifications to the police.

The sharing of information by the reporting party with other third parties	Universities must consider that any information shared with the reporting party will fall outside of the relevant university's control and may be shared with the reporting party's colleagues, friends, members of the public or even the press. Similarly, this may be the case with information shared with the responding party about the reporting party. In either case, only information strictly necessary to achieve the purpose and objective of the sharing, and that is proportionate and appropriate to share on balance in consideration of all of the factors in the **Data Sharing Impact and Risk Assessment**, should be shared. The impact of this potential wider sharing upon all the individuals involved must be considered, as such sharing of information could have a detrimental impact on their personal and/or professional lives, as well as their mental health and wellbeing. Universities could be liable under both the data protection legislation and other laws and regulations for the damage caused by such onward sharing if it can be shown that the university breached its legal obligations through the sharing of such personal data. This highlights the need to ensure that information is limited to what is necessary and factually accurate, and that any decision is documented so that the university can demonstrate how it has discharged its obligations under the data protection legislation. The decision to share any information about a disciplinary process should always, therefore, be considered in the context of who else the information could be shared with and whether the sharing is still justifiable. In any event, it is unlikely to be appropriate to share much information with a reporting party, except where strictly necessary as part of the proceedings (for example, to verify facts in the interests of a fair and thorough investigation), until the disciplinary proceedings are at a close.

Sharing information when a responding party leaves before an investigation takes place	Where a responding party leaves before the investigation takes place, they may not have responded to allegations made against them, and no outcome or sanction may have been decided upon. This scenario is considered further in UUK's guidance **Changing the culture: tackling staff-to-student sexual misconduct** (UUK 2022), where universities are advised to complete an investigation as fully as possible and to make a finding on the balance of probabilities where possible. If the university is able to carry out an investigation and make a finding on the balance of possibilities, it may be possible for the university to inform the reporting party of the outcome of their complaint, in consideration of all of the factors outlined in the Data **Sharing Impact and Risk Assessment**. However, it is unlikely a sanction would be able to be imposed in such a scenario.

b. Where the reporting party does not wish to make a formal complaint or wishes to remain anonymous	
The reporting party does not wish to make a formal complaint or wishes to remain anonymous	This scenario is considered further in UUK's guidance **Changing the culture: tackling staff-to-student sexual misconduct** (UUK 2022). It is important to note that: • A university may be unable to keep a record of the report, naming a responding party for a length of time if the reporting party wishes to remain anonymous or does not wish to make a formal complaint, and an investigation cannot take place. A lawful basis will need to be established for keeping a copy of the report (for example, the harm reported is so serious that it may be necessary to keep the report to allow for future investigation if more evidence comes to light). • Universities are obliged by the data protection principles to ensure the accuracy of the personal data held, which may not be possible if the report cannot be investigated. • A responding party may be able to request copies of such un-investigated reports as part of a Data Subject Access Request (DSAR). Having said this, in many cases it is likely that reports could be withheld from disclosure as part of a DSAR if there was a risk that the reporting party could be identified, and if it was unreasonable to disclose the report in the circumstances. Universities must ensure that such reports are kept secure, strictly confidential and on an auditable 'need-to-know' basis, considering the potentially significant impact of any leak of such report on all parties involved.

c. Sharing information with other organisations	
Sharing information about responding parties with third party organisations (for example, new employers)	This scenario is considered further in UUK's guidance **Changing the culture: tackling staff-to-student sexual misconduct** (UUK 2022). There is no specific legal right to a reference or legal obligation for a university to provide one. If a reference is given, duties of care apply to the recipient and the subject. In line with the Advisory Conciliation and Arbitration Service (ACAS) guidance, references must be honest, fair and accurate. References must be factual and must not be misleading, inaccurate, discriminatory or include irrelevant personal information. For example, a reference could state that an individual has been dismissed, or that an individual left during an active investigation, provided this information was based on facts. Universities should have reference policies in place to ensure a consistent approach. Universities must consider that there are well established rules around what can be included in references arising from employment law, defamation law and guidance (for example, the ICO Employment Practices Code of Conduct (Information Commissioner's Office, 2011)). It is therefore unlikely to be appropriate to share anything other than a limited purely factual reference with a new employer, as is generally accepted standard practice. Consider that special protections exist around the sharing of criminal conviction information, and there are specific rules around when employers, prospective employers and universities are able to run disclosing and barring service checks. As such, it may be difficult for a university to demonstrate that it is necessary to share information about reports relating to any criminal activity of a responding party, as there are already frameworks in place for disclosing this category of information.

d. Multiple reports	
Where several reporting parties all make separate disclosures about the same individual	Reporting parties may feel more able to come forward with reports or agree to participate in disciplinary proceedings if they are made aware of other similar complaints against the same responding party. Where this is the case, it may be possible to share some information about the existence of other similar complaints. Care would need to be taken when deciding if it is appropriate to share such information, and only limited information should be provided as is necessary and proportionate in the circumstances. For example, in some cases the objective of encouraging reporting parties to come forward may be met by saying that there are other similar reports, without giving details of such reports or in some cases even identifying the individuals involved. Consideration should also be given to the specific risks and circumstances of the case and all the parties involved. If there are other ways to encourage the reporting party to feel supported in reporting, then it may not be strictly necessary to tell them about any other reports. Universities could also consider sharing more generic information about action taken as a result of previous reports rather than the fact that specific reports were received about a staff member.

It is also important to consider that:

- The reporting parties may share more widely that multiple reports have been raised, and any messaging would need to be carefully managed.
- Through sharing details of another complaint with a reporting party, the university may be disclosing the personal data of another reporting party, which could end up being shared more widely. This is a particular concern where other reporting parties have sought to remain anonymous or wish for their complaint to be handled with special care for a particular reason, for example where there are safety concerns.
- Any such sharing of the existence of other complaints is likely to have a significant impact on the responding party, particularly if the information is shared more widely, both personally and professionally. Consider that the reports will not have been investigated at this stage.

Annexe 1: Establishing a lawful basis

Universities must establish a **lawful basis** under the data protection legislation to share or otherwise process any personal data.

The lawful bases for processing personal data are set out in **Article 6 of the UK GDPR**, and **Article 9 of the UK GDPR** and **Schedule 1 of DPA 2018** for special categories of personal data and criminal convictions data.

This Annexe 1 includes information on the lawful bases, which are most likely to be relevant in respect of the sharing of personal data by universities in connection with harassment cases.

Section 2 outlines a suggested framework to test whether the data sharing is **truly necessary for the purposes of the identified lawful basis** and whether the **sharing is justified in the circumstances**. Further guidance on lawful bases under the UK GDPR is available at the ICO's website (www.ico.gov.uk).

Legal obligation (Article 6(1)(c))

The data protection legislation does not automatically take precedence over other legislation or laws.

Where a university is legally required to share personal data under a separate law, it is permitted to do so under Article 6 of the UK GDPR provided such sharing is necessary. To rely on this lawful basis, the university would need to be able to **identify the specific legal obligation** which requires the sharing of the personal data.

For example, if a harassment case is also being investigated by the police as a criminal offence, the police may secure a court order requesting copies of all information that the university holds in connection with that case, and the university would be legally obliged to comply with such order. This lawful basis may also be relevant if the harassment case forms part of employment tribunal proceedings, where the university would be obliged to disclose information in connection with the case in line with the tribunal's disclosure procedures. This is also relevant, for example, where a university is legally required to refer information under its Prevent duties as set out in the Counter-Terrorism and Security Act 2015.

Performance of public task (Article 6(1)(e) UK GDPR)

As public bodies, universities may be able to demonstrate that the sharing of information in respect of harassment cases is necessary for the purposes of performance of its public tasks.

This would apply where the university is able to demonstrate that the sharing is necessary for the purposes of providing higher education services to students in a safe environment. This might apply, for example, where a university wants to reassure a student of their safety by confirming that an individual will no longer be on campus.

This lawful basis is most likely to be relevant in respect of an institution's relationship with its students, as opposed to its staff, where the relationship is more private by nature.

A university must also ensure that the sharing activity is necessary in connection with the specific public task, in particular considering the objectives and proportionality of the sharing. If there is another way to achieve the same result, the university cannot rely on public task as a lawful basis.

When relying on public task as a lawful basis, a university will need to be able to specify the particular public task and its basis in common law or statute.

Legitimate interests (Article 6(1)(f) UK GDPR)

As public bodies, universities may only rely on legitimate interests as a lawful basis for sharing personal data in limited circumstances. A university may be able to rely on this lawful basis if it is able to show that the sharing of personal data does not relate to the performance of its public tasks. This is most likely to be relevant in respect of an institution's relationship with its staff.

To rely on legitimate interests as a lawful basis, universities must:

(a) identify a genuine legitimate interest or **purpose** for sharing the information

(b) demonstrate that the sharing of the information is genuinely **necessary** to achieve the purpose

(c) conduct a balancing exercise to consider the interests or fundamental rights and freedoms of the affected individuals, and whether these override the identified purpose (**balancing test**)

This might apply, for example, where an institution wants to reassure a staff member of their safety by confirming that an individual will no longer be on campus.

Where relying on this lawful basis, universities will need to conduct a legitimate interests assessment to document how the above tests have been applied and how the decision to share personal data has been reached.

Section 2 sets out an adapted version of the ICO's legitimate interests assessment (Information Commissioner's Office, 2018), which has been expanded to reflect the specific considerations of universities in respect of harassment cases and considerations from the ICO's Data Sharing Code of Practice (Information Commissioner's Office, 2021).

The assessment tool in Section 2 can be used by universities when relying on any lawful basis to test whether the sharing is genuinely necessary and justified in respect of the applicable lawful basis.

Performance of a contract (Article 6(1)(b) UK GDPR)

The basis of a university's relationship with both its students and staff originates primarily from contract. As such, a university will be able to share personal data in respect of harassment cases where it is able to demonstrate that this is **necessary in respect of the performance of its contract** with the relevant data subject.

For example, it is necessary, as part of the effective management of contracts between a university and staff members/students, for a university to share information with the individuals responsible for conducting disciplinary proceedings so that incidents can be properly investigated, and appropriate sanctions given.

However, simply adding a clause into staff/student contracts to say that details of any outcomes or sanctions imposed against them will be shared with reporting parties is not sufficient to satisfy this lawful basis alone. The sharing would need to be strictly **necessary** for the performance of the overall contract with the data subject in question (ie the staff/student responding party).

Such sharing would also need to be fair and lawful in line with the principles of the data protection legislation (see Annexe 2) , which it may not be on consideration of the facts, even if a clause has been added to the staff/student contract. The guidance recognises that updating all student and staff contracts, particularly those with current staff and students, is unlikely to be a straightforward or manageable task for universities.

The sharing of personal data would need to be necessary for the university to comply with its obligations under the contract or for the individual to comply with their obligations under the contract. If there is another way that the specific contractual purpose can be achieved without sharing the personal data, the university will not be able to rely on this lawful basis.

Other lawful bases

Other lawful bases under the UK GDPR include:

(a) where the relevant data subject has given their consent to the sharing of their personal data

It is unlikely that a university would be able to rely on consent as a lawful basis to share information in relation to outcomes and/or sanctions. Consent must be freely given, specific and informed, and can be withdrawn at any time. There is a potential inherent imbalance of power between the university and the relevant data subjects, as this imbalance may mean, depending on the circumstances, that the consent is not freely given. In the context of staff in particular, it is rarely possible to rely on consent as a lawful basis as it is unlikely to be freely given considering the imbalance of power between a staff member and their employer. Further, consent can be withdrawn at any time, which would be almost impossible to enforce if personal data had already been shared with another individual; and

(b) where the sharing is necessary to protect the vital interests of the data subject or another individual

This is typically used in emergency purposes; for example, where it is necessary for a university to share personal data to aid an individual whose life is in immediate danger.

ICO Data Sharing Code of Practice

In its Data Sharing Code of Practice (Information Commissioner's Office, 2021), the ICO lists a number of considerations to be taken into account at the outset of any data sharing, when deciding whether or not to share personal data. For example, controllers are directed to consider the objective of the sharing, the impact of the sharing and the impact of not sharing. The assessment outlined in Section 3 directs universities to take into account these considerations when deciding whether to share personal data in respect of harassment cases.

Data Sharing Impact and Risk Assessment

UUK recommends that universities use the assessment tool in Section 2 to assess whether, on balance, it is necessary and appropriate to share personal data in connection with the performance of a contract, the performance of a public task or any other relevant lawful basis, in addition to where legitimate interests are relied upon. Universities may decide to use the tool only for the most complex cases, or for categories of cases (provided that individual cases are still considered on their facts).

The assessment tool at Section 2 also includes the considerations set out by the ICO in its Data Sharing Code of Practice (Information Commissioner's Office, 2021), and gives Universities a framework by which to document why the sharing is genuinely necessary, and the specific lawful basis relied upon, in line with the accountability principle (Article 5 UK GDPR).

Special categories of personal data

Special categories of personal data are defined in **Article 9 of the UK GDPR** as personal data relating to:

(a) racial or ethnic origin

(b) political opinions

(c) religious or philosophical beliefs

(d) trade union membership

(e) genetic data and biometric data, for the purposes of uniquely identifying a natural person

(f) data concerning health

(g) data concerning a natural person's sex life or sexual orientation

The processing of special categories of personal data is generally prohibited by Article 9 of the UK GDPR, unless one of the conditions in Article 9 or Schedule 1 of the DPA 2018 applies.

Similarly, processing of personal data relating to criminal convictions and offences is only permitted in a limited set of circumstances as outlined in Article 10 of the UK GDPR and Schedule 1 of the DPA 2018.

For ease of reference, a summary of the Article 9, 10 and Schedule 1 DPA 2018 conditions that are most likely to be relevant is set out in Annexe 2 of this guide.

Article 9 of the UK GDPR applies in addition to Article 6 of the UK GDPR, meaning that where a special category personal data or criminal convictions data is to be processed, an Article 6 lawful basis must be identified, as well as one of the conditions in Article 9 together with any associated conditions set out in Schedule 1 of the DPA 2018, where required.

The inherent nature of harassment cases (particularly racial and sexual harassment cases) is such that the information provided by the reporting party and the responding party, and any other information collected, is likely to include special categories of personal data and/or criminal convictions data.

It may be necessary for the university to share special categories of personal data and/or criminal convictions data in limited circumstances; for example, to allow a thorough investigation process. It may also be necessary, depending on the specific circumstances, to share certain information with a third party, such as the OIA, SPSO, NIPSO where the complaint is escalated to one of these bodies and specific information needs to be shared so that the relevant ombudsman can carry out its functions in investigating the complaint. In these circumstances, the university would need to establish both an Article 6 and Article 9 lawful basis to share the personal data, and, as always, the personal data shared would need to be limited to what is genuinely necessary for the specific and identified purpose.

Additional care and caution must be taken when sharing special categories of personal data or criminal convictions data, considering the sensitivity of the information.

The university will need to document the specific Article 9 and, where relevant, Schedule 1 DPA 2018 condition for sharing this personal data and why such sharing is strictly necessary, and may also need to carry out a DPIA.

This guidance does not envisage many scenarios where it is likely to be appropriate to share special categories of personal data or information relating to criminal convictions relating to a responding party with a reporting party or other third party (eg another university) in a harassment case, except in exceptional circumstances. Having said this, it is unlikely that an outcome or sanction in a harassment case would constitute a special category of personal data or criminal convictions data.

Set out below is a **summary of those conditions that might be most relevant to universities in the context of sharing personal data in relation to harassment cases**.

Please see Article 9 or 10 of the UK GDPR, Schedule 1 of the DPA 2018, and the ICO's website (www.ico.gov.uk) for further information.

Special categories of personal data	
Article 9 UK GDPR: conditions that are potentially relevant	1. The processing is necessary for the purposes of carrying out obligations or exercising specific rights in relation to employment, social security and social protection law (see also Schedule 1 Part 1 DPA 2018) 2. The processing is necessary for reasons of substantial public interest (see Schedule 1 DPA 2018, Part 2) 3. To protect the vital interests of the data subject or another individual where the data subject is not able to give consent 4. The information has been made manifestly public by the data subject 5. The processing is necessary for the establishment, exercise or defence of legal claims
Schedule 1 DPA 2018, Part 2: conditions that are potentially relevant	1. The processing is necessary for the prevention or detection of an unlawful act, must be carried out without the data subject's consent and is necessary for reasons of substantial public interest 2. The processing is necessary for the purposes of making a disclosure under terrorist finance or money laundering legislation 3. The processing is necessary for the purposes of safeguarding children and individuals at risk, where consent cannot be obtained from the data subject, and where necessary for reasons of substantial public interest
Criminal convictions data	
Article 10 UK GDPR: conditions that are potentially relevant	1. Processing is only permitted where authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects

Schedule 1 DPA 2018, Part 3: conditions that are potentially relevant	1. The processing is necessary for reasons of substantial public interest (see Schedule 1 DPA 2018 Part 2) 2. To protect the vital interests of an individual and the data subject is unable to give consent 3. The information has been made manifestly public by the data subject 4. The processing is necessary for the establishment, exercise or defence of legal claims

Annexe 2: Sharing in line with the principles

Where a university has established a lawful basis for sharing personal information in connection with a harassment case, it must ensure that it is able to perform such sharing in accordance with the principles set out in Article 5 of the UK GDPR (subject to a limited number of exceptions, where exemptions set out in Schedule 2 of the DPA 2018 apply).

Universities must ensure that any personal data in connection with harassment cases is shared in line with the following principles.

Principle	Some suggested actions
Lawful, fair and transparent	• Where appropriate, carry out the Data Sharing Impact and Risk Assessment in Section 2 to consider whether, on balance, the sharing is fair, and identify a lawful basis. • Consider the wider regulatory framework (for example, employment law, criminal law, defamation law, confidentiality, human rights laws, principles of natural justice). The decision to share or not to share the personal data must not breach any other laws. • Update privacy notices and develop and/or amend relevant policies to notify staff and students that information could be shared in relation to disciplinary cases in certain circumstances, and in line with the data protection legislation. • Keep those involved in any harassment cases, either as a reporting party, witness or responding party, informed from the outset as to the process and if and when information might be shared, to manage expectations. Ensure that the university is acting consistently in its decision-making processes regarding how to share personal data, notwithstanding that decisions need to be made in consideration of the specific facts of the case.
Limited in purpose	• Be clear about the purpose of the sharing, and clearly document its objectives. The tool in Section 2 will assist with this.

Limited to what is necessary	• Where appropriate, use the tool in Section 2 to determine which information it is genuinely necessary to share and clearly linked to the objective of the sharing. For example, it might be necessary on the facts to let a reporting party know that an individual will no longer be on campus to ensure that the reporting party feels safe and able to return. However, it may not be necessary to tell the reporting party that the individual was dismissed or to otherwise give information as to the sanction given. The decision as to what is necessary to share should be carefully considered, as set out in Section 2.
Accurate	• Ensure that any information shared is not incorrect or misleading, and carefully consider what is appropriate to share. • Ensure that thorough investigations are carried out in accordance with the relevant university's policies, sector guidance and the wider regulatory framework. • Take appropriate steps to verify and check any information where possible. • If the university decides that there are grounds to release information about an outcome of a disciplinary process, check and verify what that outcome is with those leading the investigation and disciplinary processes, and consider who should be relaying this information in accordance with the university's internal governance procedures. Consider that it may be a challenge to rectify any inaccurate information with an individual after this is shared with them, and the sharing of inaccurate information could have serious consequences. Care must therefore always be taken to ensure accuracy, and information shared should be limited to what is necessary (see above).
Not kept for longer than is necessary	• Consider that the university is unable to go back and delete any information that has been shared with an individual in a personal capacity, and this information is now outside of the university's control. • Universities must be able to justify how long it is holding personal data in line with the purpose for which it was collected, and will need to document this in its privacy policies.

Security	• Consider that once information is shared with an individual in a personal capacity, the university will lose control of that information and will no longer be able to ensure its security. As such, information shared should be limited to what is necessary (see above). • Consider that only university staff who need to know the information (e.g. HR professionals, disciplinary investigators) should have access to the information • Consider appropriate cyber security measures. The National Cyber Security Centre has guidance for the education sector
Accountability	• Where appropriate, use the tool in Section 2 to decide and document whether, on balance, it is appropriate and in line with the data protection legislation and wider regulatory framework to share personal data in relation to harassment cases. • Carry out a DPIA if appropriate. • Ensure that privacy notices and any other relevant policies outline how and when information might be shared in connection with disciplinary cases in certain circumstances, and in line with the data protection legislation.

Annexe 3: Obligations

When sharing any personal data in connection with harassment cases, universities will need to ensure that they comply with their obligations under the data protection legislation, as they would in respect of any other activity involving the processing of personal data.

In particular, universities must ensure that data subjects can exercise their rights (Articles 12–22 inclusive, UK GDPR).

This Annexe sets out several obligations that may be relevant to harassment cases. **However, this is not an exhaustive list and universities will need to seek separate advice in respect of their obligations under the data protection legislation**.

Transparency

Universities should update privacy notices and develop/amend other relevant policies to comply with transparency obligations (Article 13 and 14, UK GDPR), specifying how and when personal data, including outcomes, may be shared in respect of disciplinary proceedings, grievances and complaints, where appropriate in line with the data protection legislation.

Data Subject Access Requests (DSARs)

Universities must bear in mind that data subjects are able to request access to their personal data, subject to exemptions (for example, where information relates to a criminal investigation and releasing such information would prejudice that investigation, or where the information contains personal data of another person, and it would be unreasonable to share such information).

This might be relevant, for example, if the responding party makes a DSAR in connection with the wider disciplinary proceedings, in which case universities will need to consider what information the responding party is entitled to as part of their DSAR under the data protection legislation. In particular, universities will need to consider whether it is appropriate to disclose personal data of other data subjects to the responding party making the DSAR, considering whether those other data subjects have consented to such disclosure, whether redactions can be made to remove personal data, or whether the disclosure is reasonable in the circumstances (Section 16, Part 3, Schedule 2 DPA 2018).

UUK has been made aware of reports that reporting parties have been using DSARs to attempt to access information about outcomes and sanctions relating to their report and the associated disciplinary processes. As reporting parties are only entitled to request copies of their own personal data in a DSAR, it is unlikely that they would be entitled to request information about sanctions, as such information is the personal data of the responding party. , This demonstrates the importance of being transparent, and sharing information about outcomes and, where possible, sanctions where lawful to do so to avoid an increase in DSARs from reporting parties, and the additional administrative burden that these place on both the reporting party and the university.

Universities will need to consider that data sharing and the disclosure of information may take place across a number of different processes in connection with harassment cases, including in respect of the investigation, disciplinary or complaints process, and if a data subject makes a DSAR. **Universities will need to take a cross-departmental approach to maintain oversight over the decisions being made in relation to data sharing across different processes**, to ensure that any data sharing is consistent and remains within the confines of the data protection legislation and the wider regulatory framework.

Data Protection Impact Assessment (DPIA)

Although most data sharing relating to harassment cases will be on an ad hoc, case-by-case basis, it may be appropriate in some circumstances for universities to carry out a DPIA in respect of such data sharing. Similarly, it may be appropriate for universities to conduct a more general DPIA in relation to the sharing of personal data in connection with student and staff disciplinary proceedings.

The ICO recommends that the DPIA process is always considered as a first step where personal data is shared (Information Commissioner's Office, 2021, p. 20), and the relevant individuals within a university who manage harassment cases should liaise with their data protection officers (DPOs) to discuss where a DPIA may be appropriate.

A DPIA will consider the potential impact of the sharing or processing activity on the data subject, including any risks and how these might be mitigated.

A note on exemptions

This guidance does not explore the exemptions set out in Schedule 2 of the DPA 2018 in detail, and universities are encouraged to visit the ICO's website for further information (www.ico.gov.uk). However, this guidance recognises that it is a common misconception that the Crime and Taxation Exemption (Section 2, Part 1, Schedule 2 DPA 2018) provides a lawful basis for the processing and sharing of personal data in connection with the prevention or detection of crime, which is not correct.

The exemptions set out in Schedule 2 of the DPA 2018 apply in relation to a university's obligations under the Data Protection Legislation, and exempt the university from complying with some of those obligations in limited circumstances. The exemptions are not lawful bases, and a university would still need to establish a lawful basis under Article 6, and where appropriate satisfy a condition under Articles 9 or 10 if special category or criminal convictions data is being processed, (see Annexe 2) to process/share personal data.

For example, in relation to information requested by the police, the lawful basis could be that the sharing is necessary to comply with a legal obligation where there is a court order or warrant (Article 6(1)(c)) or there is some other reason why the sharing is necessary in connection with the university's public task (Article 6(1)(e)) or legitimate interests (Article 6(1)(f)). For further information on sharing information with law enforcement authorities, please see the ICO's guidance.

References

- ACAS (2019) Conducting Workplace Investigations
- ACAS (2020) Discipline and Greivances at Work
- Bradfield N, Pinsent Masons (2016) Guidance For Higher Education Institutions: How To Handle Alleged Student Misconduct Which May Also Constitute A Criminal Offence
- EHRC (2019) Tackling racial harassment: Universities challenged
- ICO (2011) The Employment Practices Code
- ICO (2018) Sample LIA Template
- ICO (2020) Age appropriate design: a code of practice for online services
- ICO (2021) Data Sharing Code of Practice
- OIA (2016) The good practice framework: handling student complaints and academic appeals
- OIA (2018) Supplying Personal Data to the OIA
- OIA (2018) The Good Practice Framework: Disciplinary Procedures
- OIA (2018) Briefing Note: Complaints involving sexual misconduct and harassment
- SPSO (2020) The Model Complaints Handling Procedures
- UUK (2019) Changing the culture: tackling Online Harassment and Promoting Online Welfare
- UUK (2020) Changing the culture: tackling racial harassment
- UUK (2020) Chaaging the culture: tackling staff-to-student sexual misconduct

Universities UK is the collective voice of 140 universities in England, Scotland, Wales and Northern Ireland.

Our mission is to create the conditions for UK universities to be the best in the world; maximising their positive impact locally, nationally and globally.

Universities UK acts on behalf of universities, represented by their heads of institution.

Universities UK

Woburn House
20 Tavistock Square
London, WC1H 9HQ

+44 (0)20 7419 4111
info@universitiesuk.ac.uk
universitiesuk.ac.uk
@UniversitiesUK

May 2022
ISBN: xxxx