

# Changing the culture: sharing personal data in harassment cases

Strategic guide for universities



## Contents

---

Foreword by Professor David Richardson	1
1. Introduction	4
2. Legal and regulatory overview	16
3. Creation and maintenance of an anonymous record of reports	23
4. Next steps	26
Acknowledgements	29
Annexe 1: Glossary	31
Annexe 2: References	35

# Foreword by Professor David Richardson



An institution's response to incidents of harassment is vital. Although universities work hard to prevent harassment, we know these incidents will occur, so students and staff must have confidence that they will be dealt with fairly and effectively.

Evidence from the Equality and Human Rights Commission's (EHRC) 2019 inquiry into racial harassment revealed substantial under-reporting of racial harassment by students and staff. This reflects under-reporting of all forms of harassment across society. In particular, the EHRC found large discrepancies between the numbers of staff members and students who had experienced harassment and the numbers of formal complaints recorded by universities. Criticisms included not being believed, not feeling they are in a safe environment, not being supported and not learning the outcomes of a report.

The first three of these we can respond to by reviewing and improving our report and support processes: information on how to do this is available in Universities UK (UUK) guidance on tackling racial harassment and guidance on addressing staff-to-student sexual misconduct, both of which should be read alongside this guidance.

This guidance looks at the steps institutions should take to respond to the last issue, sharing information on outcomes in harassment cases. The rationale for doing this is obvious: it takes great courage for an individual to report an incident of harassment and receiving information on the decision made by the university can help deliver effective redress, remedy the harm caused and increase the student's feeling of safety at the university.

However, as demonstrated in the EHRC report, institutions reported that meeting data protection obligations limits their ability to share information on outcomes and sanctions in an investigation and disciplinary process with the reporting party. Therefore I have been pleased to oversee the work of this guidance to increase the understanding around when data can be shared, and to support effective complaints handling and redress for victims-survivors.

This guidance has been prepared to empower universities to make informed, pragmatic and considered decisions as to whether to share personal data. We hope this will support a shift in institutional culture by improving how harassment cases are handled, in a more transparent and satisfactory way for all parties involved. The guidance encourages institutions to move away from blanket refusals to share personal data, towards taking more case appropriate decisions to share personal data while complying with current data protection legislation.

In some cases, it will be clear whether information on outcomes can be shared with reporting parties. However, in more complex harassment cases this can be much more difficult. This guidance is designed to support universities to respond to those more complex cases. To do this, we provide a **Data Sharing Impact and Risk Assessment**, which is set out in the **Practical guide** accompanying this Strategic guide. This assessment tool guides universities through the decision-making process, balancing the competing interests of affected individuals, so that universities can arrive at, and document, a decision that is appropriate for the specific circumstances and fair and balanced for all.

The implementation of this guidance will require the buy-in from various teams and departments across universities, particularly members of staff who handle complaints and grievances on a day-to-day basis, as well as data protection officers (DPOs). To ensure commitment to moving from blanket decisions to more pragmatic case-specific decisions, it is also important for sector leaders to promote this guidance. In particular, I urge leaders to promote:

- moving away from the assumption that data protection legislation always prevents sharing of personal data and for universities to consider the circumstances when it is appropriate and lawful to share personal data
- moving towards more pragmatic, informed and considered decisions to share personal data in relation to harassment cases, which should be made on a case-by-case basis
- more transparency in how harassment cases are handled, including the management of expectations of all those involved, and the sharing of personal data in accordance with data protection legislation and the wider regulatory framework

While developing this guidance, UUK spoke with many different groups. What became immediately clear was that views varied across different teams and groups within universities in terms of what universities could do. Some universities already felt confident, within the current legislative framework, to provide information on outcomes and sanctions of disciplinary processes to reporting parties in many cases. Others felt constrained by data protection legislation.

In writing this guidance, we have tried to take account of these differing views and hope that the information we provide on the benefits of sharing information will help inform conversations across different groups when considering whether to share information.

Given the difference in approaches, UUK also met with the Information Commissioner's Office (ICO) and the EHRC to seek further clarity and advice as the guidance was developed, and to raise awareness of the concerns brought to UUK's attention from different groups.

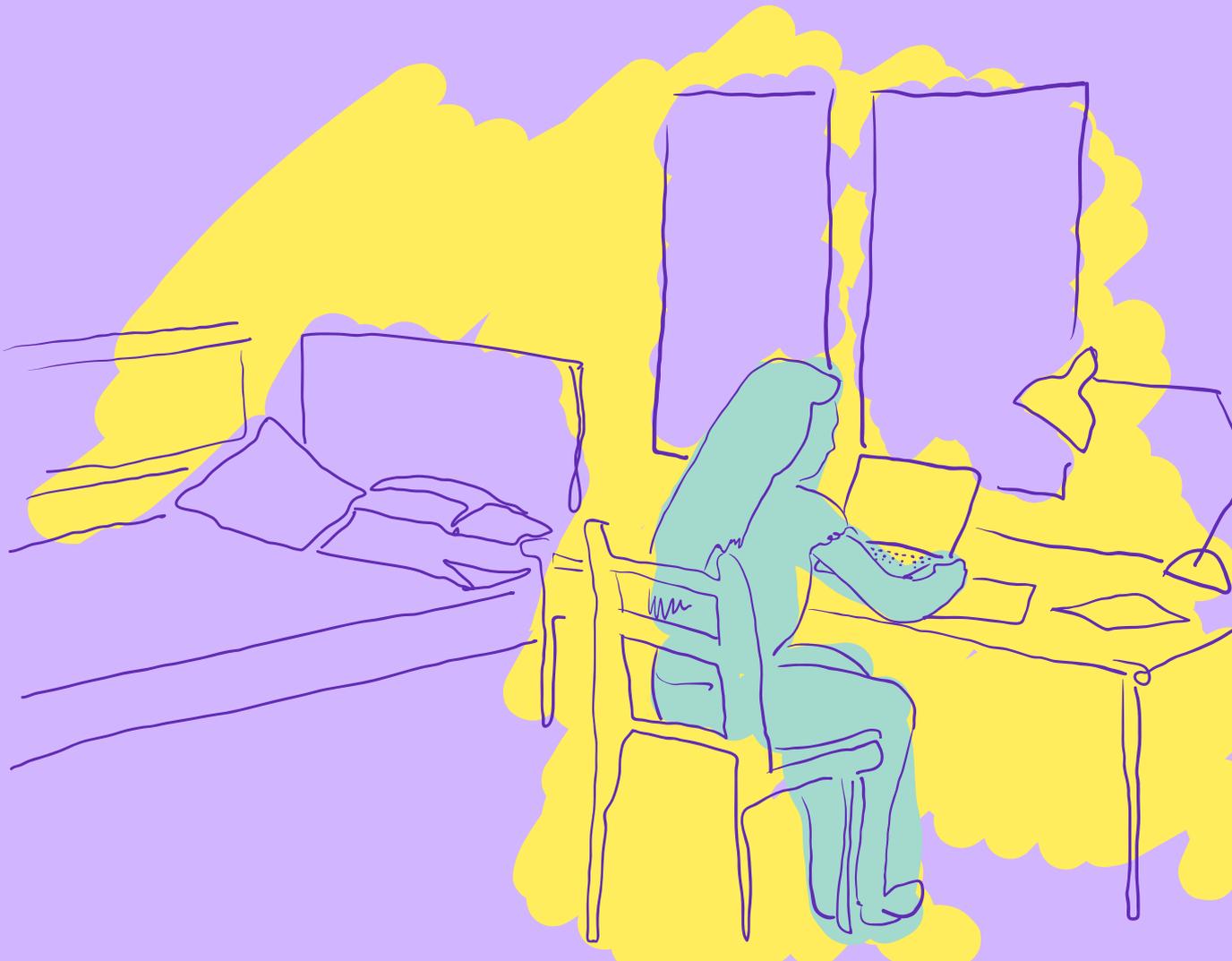
UUK recognises that this guidance is a 'living' document. As such, we will engage with universities over the coming 12 months to understand how this guidance has been used and implemented. This will be followed by a full review in 2023 and may be updated as new issues arise or to provide further clarification.

UUK has consulted with the ICO on this version of the guidance and the regulator has welcomed the framework as a mechanism that can support universities in deciding whether to share personal data. I commend this guidance to you and hope that this will support your institution to take steps to share information and increase transparency for reporting parties, where appropriate, proportionate and lawful to do so, bearing in mind the need to balance the rights of both the reporting and responding parties.

Finally, I am most grateful to all the members of UUK's Advisory Group and Wider Stakeholder Group for contributing their time and expertise to the development of this guidance. Particular thanks go to Elizabeth Dunford, Principal Solicitor (Technology/Data Protection) at Coventry University who has prepared and written this guidance for the higher education sector.

**Professor David Richardson, Vice Chancellor of the University of East Anglia,  
Chair of Universities UK Wider Stakeholder Group**

# 1. Introduction



Sharing data in harassment cases was identified as a key challenge for universities by the Equality and Human Rights Commission (EHRC) in their inquiry into racial harassment in higher education in 2019. Responding to this, Universities UK (UUK) was tasked by the EHRC with working with the sector, the Information Commissioner's Office (ICO) and data protection officers (DPOs) to develop sector guidance to **increase understanding around when it is appropriate to share personal data when managing harassment complaints**. Evidence from the inquiry found some universities were reluctant to share information on outcomes and sanctions of an investigation or disciplinary process with reporting parties due to fears this would breach data protection legislation.

“Overall, our evidence showed many universities were taking a risk-averse approach, preventing them from addressing harassment in individual cases and at a broader, institutional level.”

EHRC (2019), p79

The EHRC expressed concern that such a ‘risk-averse approach’ hindered an institution’s ability to deliver **effective redress** to those making a complaint. This could **act as a barrier** to encouraging students and staff to report. This also represented a **missed opportunity** by the university to promote the consequences of unacceptable behaviour more widely and increase the confidence students had in the university’s complaints system.

Frontline practitioners and campaigners have expressed similar concerns to UUK around the **lack of transparency** by universities in sharing outcomes and sanctions with reporting parties in cases of sexual misconduct and harassment.

“When it comes to data sharing, reporting students are telling us that the withholding of key information doesn’t feel fair and balanced to them; they’re telling us that not sharing information is having a detrimental impact on their mental health, their ability to feel safe on campus, and their ability to continue with their education.”

Dr Kelly Prince, Independent Researcher, and former Serious Incident Case Officer in Higher Education.

## Purpose

In 2020, UUK established a stakeholder group, chaired by Professor David Richardson, Vice-Chancellor of the University of East Anglia, to develop guidance to support universities:

- a. to have the confidence to share more information on outcomes and sanctions with reporting parties where it is appropriate and reasonable to do so
- b. to move away from blanket policies to either always refuse or always allow the sharing of personal data in harassment complaints, investigations and disciplinary proceedings, so that each case can be handled appropriately on its specific facts
- c. by raising awareness of the benefits of sharing more information with reporting parties to inform and support conversations between frontline practitioners supporting students, staff working on complaints and DPOs
- d. by providing a framework to support universities in their decision-making process taking account of legal, regulatory, policy and wellbeing reasons for sharing data
- e. in identifying specific situations where it may be appropriate to share information on outcomes and sanctions in complaints, investigations and disciplinary proceedings, where it is reasonable to do so

## How universities should use this guidance

The guidance is aimed at:

- staff handling harassment and misconduct complaints and reports from both staff, students and third parties
- members of disciplinary panels when deciding what information to share about an outcome or sanction, as appropriate and where lawful to do so
- DPOs, to continue to provide guidance and assistance, particularly in cases where the decision to disclose or withhold personal data is not clear
- senior leadership teams, who will need to encourage within their institutions a culture change away from the application of blanket policies to share/not to share

The guidance is split into two parts: this Strategic guide, and a Practical guide.

- This Strategic guide outlines the underlying principles and themes of the guidance. This will be most useful for those leading on strategies to tackle harassment, such as senior leadership teams.
- The Practical guide sets out the technical elements of this guidance, including the Data Sharing Risk and Impact Assessment. This will be most useful for those working on harassment cases on a day-to-day basis, who will be regularly making decisions as to whether to share personal data.

## Underlying principles

The guidance follows several underlying principles. These can be applied to any sharing of personal data in connection with harassment cases, misconduct cases or otherwise.

<p><b>Data protection legislation is not a barrier to data sharing</b></p>	<p>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.</p>
<p><b>Data protection legislation should be considered in the context of the wider regulatory framework</b></p>	<p>Data protection legislation does not automatically take precedence over other legislation and is designed to work with and complement other legislation. Data protection legislation specifically allows for personal data to be shared in circumstances where this is necessary to comply with another legal obligation.</p> <p>Universities should also consider the wider regulatory framework when deciding whether to share personal data.</p>
<p><b>Rights granted under data protection legislation apply equally to both the reporting party and the responding party</b></p>	<p>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.</p>

<p><b>Decisions must be made on a case-by-case basis and on the facts of the case</b></p>	<p>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.</p> <p>The Practical guidance provides a proposed framework for universities to follow when approaching decisions to share personal data in harassment cases. The tool is aimed at guiding universities through the decision-making process but cannot advise an institution as to what the decision should be.</p>
<p><b>Universities must decide how best to implement this guidance</b></p>	<p>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.</p>
<p><b>Transparency</b></p>	<p>To be effective in encouraging reporting parties to come forward, the outcome to a complaint should be as transparent as possible.</p> <p>Universities should maintain communication with all parties throughout the handling of harassment cases, sharing information where appropriate and lawful in accordance with 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.</p>

The guidance recognises that there are many situations where from the outset it will be clearly appropriate to share some personal data such as:

- where there is already a clear legal obligation to share the information (for example, where there is a court order to release information)
- in widely established practices (for example, in the context of employment law)
- where there is a genuine and immediate threat to life
- in the case of fitness to practice processes and procedures by a university or appropriate regulatory body

There will, however, also be situations where **it may not be clear whether personal data should be shared**. This is particularly likely when the case is **complex** with multiple considerations on both sides, and it is necessary to probe the facts of the case to see if it is appropriate to share on balance. **This guidance supports universities to respond to these cases.**

Examples of common scenarios where this is likely to be the case are explored further in the Practical guide [Section 3](#).

The guidance has been developed to be read alongside other UUK reports that refer to all stages of the complaint process:

- [UUK's Guidance to tackle racial harassment](#)
- [UUK's Strategic guidance to address staff-to-student sexual misconduct](#)

## Format of the guidance

This **Strategic guide** is structured as follows:

- [Section 1](#) provides an overview and introduction to the background, format and key themes of the guidance.
- [Section 2](#) outlines the legal and regulatory framework that universities must consider when using the guidance.
- [Section 3](#) contains guidance on the creation and maintenance of anonymous reporting records.
- [Section 4](#) outlines the high-level next steps for universities following the publication of the guidance.
- [Annexe 1](#) outlines a glossary of terms.
- [Annexe 2](#) sets out the references which underpin the guidance.

The accompanying **Practical guide** is structured as follows:

- Section 1 sets out how to use the guidance.
- Section 2 provides the Data Impact and Risk Assessment, which is a tool to support universities when deciding whether to share personal data and for documenting such decisions.
- Section 3 offers considerations for specific scenarios that have been highlighted as frequently asked questions throughout the preparation of the guidance.
- Annexes 1–3 provide detail around the application of the data protection legislation underpinning both the Strategic and Practical guide.

## The focus of this guidance

The Practical guide focuses primarily on **sharing personal data on outcomes and/or sanctions imposed in harassment complaints, investigations and disciplinary processes.**

The guidance distinguishes between **outcomes** and **sanctions**. In many cases, it will be appropriate to treat information relating to outcomes and sanctions **differently** due to the degree of sensitivity of the information to the parties involved.

### Outcomes

**Outcomes** refer to the resolution of the complaint. This could be that the complaint has been upheld, appropriate action has been taken or that a responding party will no longer be on campus.

An outcome relates to both the reporting party (as it is the outcome of their complaint) and the responding party (as it is the outcome of any investigation against them).

**Good practice states that information about outcomes should be shared with reporting parties, wherever possible and lawful to do so, so that they can see that their complaint has been dealt with and investigated.**

This is also in line with guidance from:

- the Office for the Independent Adjudicator (OIA)
- the Scottish Public Sector Ombudsman (SPSO)
- the Northern Ireland Public Sector Ombudsman (NIPSO)
- ACAS guidance on managing sexual harassment complaints in the workplace (2021)

## Sanctions

A **sanction** can be imposed on a responding party as a result of a disciplinary process, and could include an apology, warning, training, dismissal or expulsion.

Sanctions imposed are personal to the responding party, and the potential impact of sharing a sanction is likely to be more significant than the sharing of an outcome, **both** to the reporting party and the responding party. Greater care must therefore be taken when deciding whether to share information about a sanction, in particular considering the potential impact of the sharing on both the reporting party and the responding party. On a case-by-case basis and where appropriate, subject to the requirements of data protection legislation, a university should consider informing the reporting party of any sanctions imposed. This reflects the approach in the [guidance](#) for employers by the Advisory Conciliation and Arbitration Service (ACAS) for handling sexual harassment complaints. This guidance states:

“You should consider on a case-by-case basis whether to tell the person who made the complaint about what disciplinary action, if any, has been taken. You should tell them if you can.”

However, notwithstanding the information above, the situations in which details of sanctions can be shared are likely to be more limited.

In general, it would not be expected that a disclosure of a disciplinary outcome would set out detailed information about the nature of a sanction or penalty. Rather, in many cases and depending on the circumstances, it may be appropriate for the reporting party to be told that sanctions had been applied or that a penalty had been imposed. It may, however, depending on the circumstances, be appropriate to share some information about a sanction imposed; for example, if part of the sanction is a no-contact order, which the reporting party would need to be aware of in order to alert the institution to any breaches of that order.

## Approaches across the sector

From the outset, it was clear when preparing the guidance that approaches to sharing information relating to outcomes and sanctions with reporting parties differed between universities, and across different groups of staff within universities.

Although the EHRC inquiry found that many universities felt constrained to share information due to data protection legislation. Since conducting this work, UUK has found that there are a few universities that do provide information on outcomes and sanctions of disciplinary processes to reporting parties, and this is clearly set out in their institutional policies.

Given the differing views and approaches across the sector, UKK consulted with both the ICO and EHRC regarding data protection legislation. The guidance we were given clearly emphasises that **data protection legislation should not be seen as a barrier to sharing information and where legally possible, universities should share information on outcomes and sanctions with reporting parties, and that decisions to share information should be made on a case-by- case basis**. The guidance has been prepared on the basis of this underlying principle.

Universities should, where not already covered, **update their privacy notices and policies** accordingly to inform both reporting parties and responding parties that information about outcomes and sanctions may be shared depending on the circumstances.

## Why is sharing data important?

There are many reasons why it may be beneficial to share personal data:

- (i) **An effective complaints process requires transparency**, so that students and staff understand how their information will be shared. This helps students and staff to know what to expect and that the process will be conducted fairly. Increasing transparency around outcomes of complaints will encourage more people to report. OIA and SPSO guidance specifically encourages universities to identify what students want to achieve from making a complaint, at the outset, to inform them whether their expectations are reasonable and for universities to give clear reasons for the decisions they reach. UUK/Pinsent Masons Guidance on student misconduct (2016) recommends that universities publish a code of conduct and disciplinary procedures that define unacceptable behaviours and set out the likely sanctions that could be imposed on students.
- (ii) **To support the mental health and wellbeing of reporting parties** (both students and staff)
- (iii) **To provide satisfactory outcomes for reporting parties**; for example, so that the reporting party feels they have received a resolution to their complaint and that their complaint has been heard and dealt with, or to alleviate concerns they may have for their safety and that of other students and staff in the institution.

“Universities recognised that a lack of disclosure could leave students and staff dissatisfied, and unconvinced they had achieved anything by pursuing their complaint, even when their complaint is upheld.”

EHRC (2019)

- (iv) **To ensure reporting parties are aware of any sanctions placed on the responding party so they can ensure that these are being complied with.**  
For example, if a sanction has been imposed upon the responding party to prevent them from having contact with the reporting party, the reporting party needs to be informed so they know when a breach may have occurred.
- (v) **To show and promote universities’ efforts to create a positive culture.** This will enable students and staff to understand that any form of misconduct or harassment will not be tolerated, helping them to feel safe and confident to make a disclosure or report, and to understand that the institution would act when necessary.

EHRC's 2019 report **Tackling racial harassment: Universities challenged** highlighted that a practice of not sharing outcomes and sanctions of disciplinary proceedings in harassment complaints could lead to:

- mental health and wellbeing issues for reporting parties
- underreporting of incidents of racial harassment
- unsatisfactory outcomes for reporting parties
- increased likelihood of disengagement from student and working life, undermining student retention and attainment, and resulting in student reporting parties leaving education
- an impact on career development and progression of staff resulting in staff leaving employment
- a lack of confidence by students and staff that universities were taking appropriate action to tackle incidents and prevent future harassment
- concerns for safety of other students and staff
- undermining an institution's efforts to create an institutional culture that encourages students to feel safe and confident to make a disclosure or report, and to tackle racial harassment

## 2. Legal and regulatory overview



The Practical guide sets out the steps to take when deciding whether to share personal data.

At the centre of the Practical guide is the **Data Sharing Impact and Risk Assessment**. This tool walks universities through several factors to consider and balance when deciding whether to share details of an outcome or a sanction in harassment cases.

To support this process a series of questions are provided to help explore what the benefits and impact of sharing might be and where the risks are. The questions have been developed by UUK using the **ICO Legitimate Interest Assessment Guidance** and their **Data Sharing Code** (which offer universal guidance for UK organisations) as a base and take account of institutional obligations under all relevant legislation and the wider regulatory framework

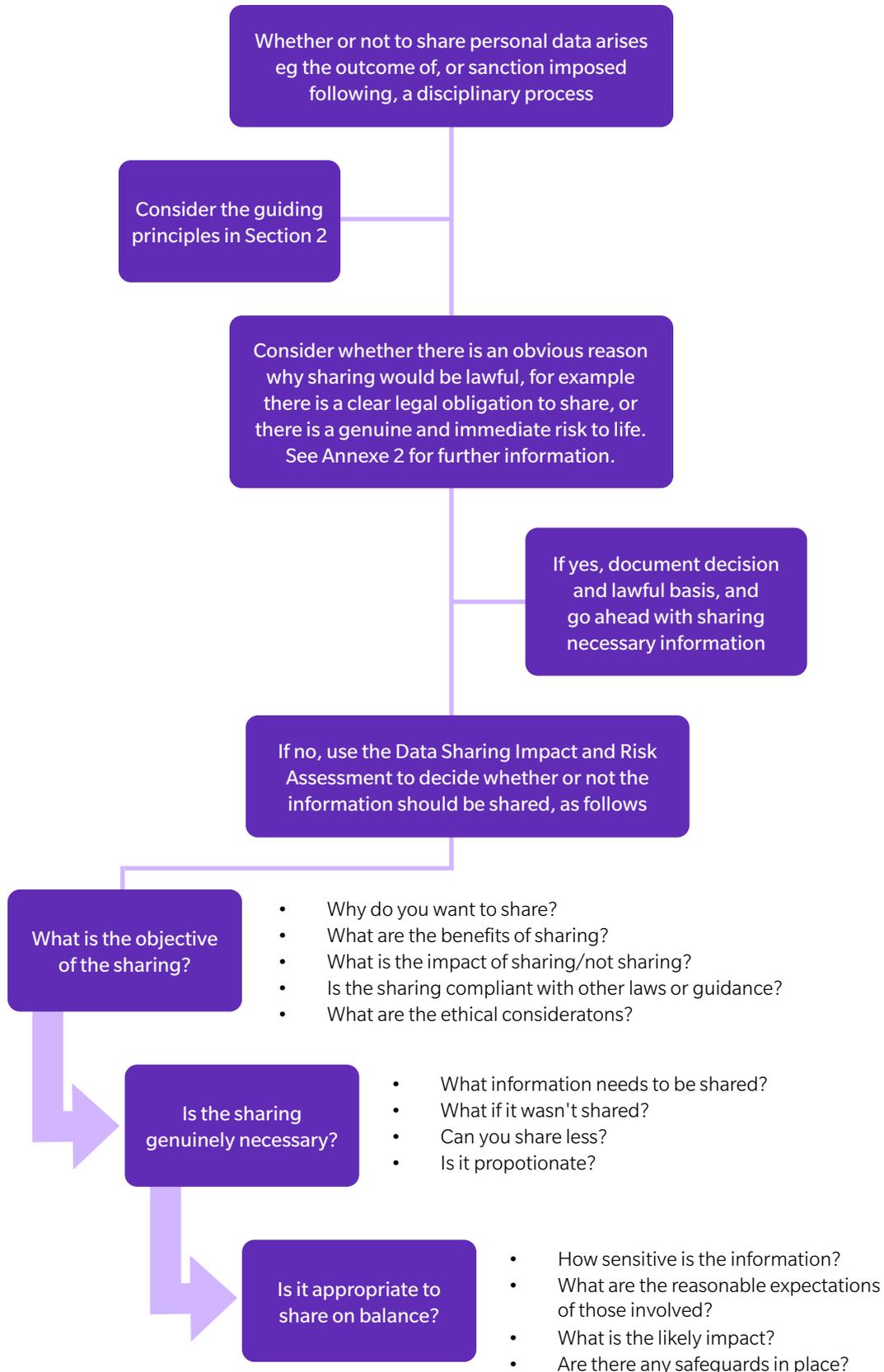
**When working through the framework, universities should consider whether their obligations to sharing the data comply with data protection legislation and other legislation, including the Equality Act 2010, Human Rights Act 1998 and common law duty of care (see Section 2 for the wider legislative and regulatory framework).**

The framework outlined in the Practical guide can be used for all **forms of harassment and misconduct** cases relating to staff, students or third parties within universities.

The **Data Sharing Impact and Risk Assessment** also provides a mechanism for universities to record their decision for audit and accountability purposes.

Details of applicable data protection law and how this applies is available in Annexes 1–3 in the Practical Guide. This also illustrates the rationale behind the **Data Sharing Impact and Risk Assessment**.

An overview of the decision-making process detailed in the Practical guide is set out in **Figure 1**.



**Figure 1.** Steps to take when deciding whether to share personal data.

When considering if it is appropriate for personal information to be shared, the obligations of the university and the rights of the individuals involved in the case must be carefully balanced according to the specific circumstances of that case.

In each case, a university must consider how the sharing of personal data and the handling of a harassment case more generally align with a university's obligations in the context of the **wider legal and regulatory framework**.

## What is personal data?

Under the data protection legislation, personal data is any information relating to an identified or identifiable living individual (Article 4(1), UK GDPR). The guidance anticipates that most information relating to a specific harassment case is likely to be personal data of the responding and/or the reporting party; for example, the outcome of disciplinary proceedings, sanctions imposed, evidence relied on throughout the investigation and in any hearing, the fact that an allegation has been made and the specific details of any allegation.

## Data protection legislation and guidance

The Data Protection Act 2018 (DPA 2018) and the UK-retained General Data Protection Regulation 2016 (UK GDPR) form the basis of the regulatory framework for the processing of any personal data within the UK (together, the 'data protection legislation').

The ICO also publishes regular guidance and codes of conduct, some of which are statutory and others advisory. In particular, the guidance refers to the:

- ICO's [Data Sharing Code of Practice](#) (Information Commissioner's Office, 2021)
- [Employment Practices Code](#) (Information Commissioner's Office, 2011) (please note that this is due to be reviewed and replaced in the near future, and such replacement versions of this code will be considered in future reviews of this guidance), and
- general guidance available at the ICO's website ([www.ico.org.uk](http://www.ico.org.uk))

Universities should also consider the ICO's recent [Age Appropriate Design: a Code of Practice for Online Services](#) (Information Commissioner's Office, 2020) when updating privacy notices, particularly in respect of providing privacy information to students and applicants who may be under 18.

The DPA 2018, UK GDPR and ICO guidance should be considered in all cases where universities make decisions on whether to share personal data in the context of harassment cases.

Data protection legislation is designed to work alongside and complement other legislation there are provisions within the data protection legislation and specifically allowing for personal data to be shared where there is a legal obligation to do so (Article 6(1)(c) UK GDPR). Whether the sharing is in accordance with other laws and relevant guidance is also a consideration when relying on other lawful bases (see Annexes 2 (Establishing a lawful basis) and 3 (Sharing in line with the principles)).

## Other relevant regulations

When deciding whether and how to share personal data in harassment cases, universities will need to **consider the wider regulatory framework** to which they are subject, considering all the relevant legislation on balance. Examples of key relevant regulations are set out below.

- (a) **Human Rights Act 1998** (HRA 1998) and **the European Convention on Human Rights** (ECHR). In particular, the right to family life (Article 8, ECHR), prohibition of discrimination (Article 14, ECHR), right to education (Article 2 of the First Protocol, ECHR).
- (b) **Equality Act 2010** (EA 2010).
- (c) **Employment law**, including the Employment Rights Act 1996, common law and applicable case law.
- (d) **Privacy law**, including the common law duty of confidentiality and the tort of the misuse of private information.
- (e) **Defamation law**.
- (f) **Criminal law**. In some harassment cases, the behaviour may constitute a criminal offence, and there may be a police investigation. Please see the **Guidance for Higher Education Institutions for further information on how to handle student misconduct cases that may also constitute a criminal offence**, and **ACAS guidance on Conducting Workplace Investigations** (2019) in respect of employees.

- (g) **Legal duties in relation to the disclosure of information**; for example, in respect of safeguarding and Prevent, including as set out in the Safeguarding Vulnerable Groups Act 2006 and the Counter-Terrorism and Security Act 2015.
- (h) **The rule of law and principles of natural justice**, in particular the right to a fair hearing and to respond to allegations, and common law duties of care including in relation to safety and welfare of staff and students (see UUK's guidance **Tackling Online Harassment and Promoting Online Welfare** (UUK, 2019) for a summary on universities' duty of care). Universities owe duties of care to both reporting and responding parties.

**The above is not an exhaustive list and universities will need to seek their own legal advice to establish the laws and regulations to which they are subject.**

## Regulatory frameworks relating to complaints

Alongside the legal framework, universities also need to consider appropriate regulatory guidance. This list is not exhaustive.

- (a) In the case of English and Welsh universities, guidance published by the **OIA**, including its **Good Practice Framework on Complaints Handling** (Office of the Independent Adjudicator, 2016), **Good Practice Framework on Disciplinary Procedures** (Office of the Independent Adjudicator, 2018) and **Supplying Personal Data to the OIA** (Office of the Independent Adjudicator, 2018); **Briefing Note: Complaints involving sexual misconduct and harassment** (2018).
- (b) In the case of Scottish universities, guidance published by **SPSO**, including its **Model Complaints Handling Procedures** (Scottish Public Services Ombudsman, 2020).
- (c) In the case of Northern Irish universities, guidance published by **NIPSO**, including its **Principles of good complaint handling**, as set out on its website (<https://nipso.org.uk/nipso/for-organisations/information-and-guidance/>).
- (d) Guidance relating to specific issues and areas, such as the **ACAS Guide to Discipline and Grievances at Work** (ACAS, 2020), **ACAS Guide to Conducting Workplace Investigations** (ACAS, 2019) and **ACAS Guidance on handling a Sexual Harassment Complaint** (ACAS, 2021).

Alongside these frameworks, universities are encouraged to refer to other guidance published by UUK. For example:

[Guidance for Higher Education Institutions](#) (Bradfield, Nicola; Pinsent Masons, 2016),

[Tackling Online Harassment and Promoting Online Welfare](#) (UUK, 2019),

[Tackling racial harassment in higher education](#) (UUK, 2019)

[Changing the culture: tackling staff-to-student sexual misconduct. A strategic guide](#) (UUK, 2022).

Changing the culture: tackling staff-to-student sexual misconduct. A practical guide (UUK, 2022).

# 3.

## Creation and maintenance of an anonymous record of reports



Recommendation six of the EHRC's report (Equality and Human Rights Commission, 2019, pp. 16, 17) recommends **that universities create and maintain an anonymous record of reports made. This is statistical data collected for reporting purposes such as; the development of reports for senior management and governing bodies, and recording trends and providing institutions with intelligence to inform their understanding of the type and scale of harassment, which will help to facilitate targeted preventive and response measures, and inform policies and general practice.**

**This is separate and distinct from creating a reporting system that allows reporting parties to make reports anonymously and universities to investigate or otherwise address anonymous reports where possible.** The creation of such a system is supported by UUK, and is addressed in more detail in [UUK's guidance on addressing staff-on-student sexual misconduct](#) and [racial harassment](#).

A record of reports made for statistical purposes should be kept anonymous, as it is not necessary to identify the individuals to which each report relates in order to run statistical reports on the data.

**Truly anonymous data is not personal data**, and therefore falls outside of the data protection legislation's scope and can be held without triggering the application of the data protection legislation.

When creating such a system for statistical purposes, it is important to ensure that the information can be recorded in a truly anonymous form. This means making sure that no individual can be identified (or re-identified) from the information retained, or by combining that information with other information which might be available (including personal knowledge of individuals), and that no references (for example, pseudonyms or reference numbers) can be used to connect data collected back to individuals.

Universities should consider **how such a statistical record should be created to ensure anonymity** and that the record is an accurate reflection of what has happened, whilst remaining anonymous. For example, universities may wish to wait until the end of a disciplinary process to add an incident to the centralised record, when a decision has been made.

Universities may also wish to determine **categories of incidents** against which reports can be recorded for reporting purposes and to review trends, whilst maintaining anonymity.

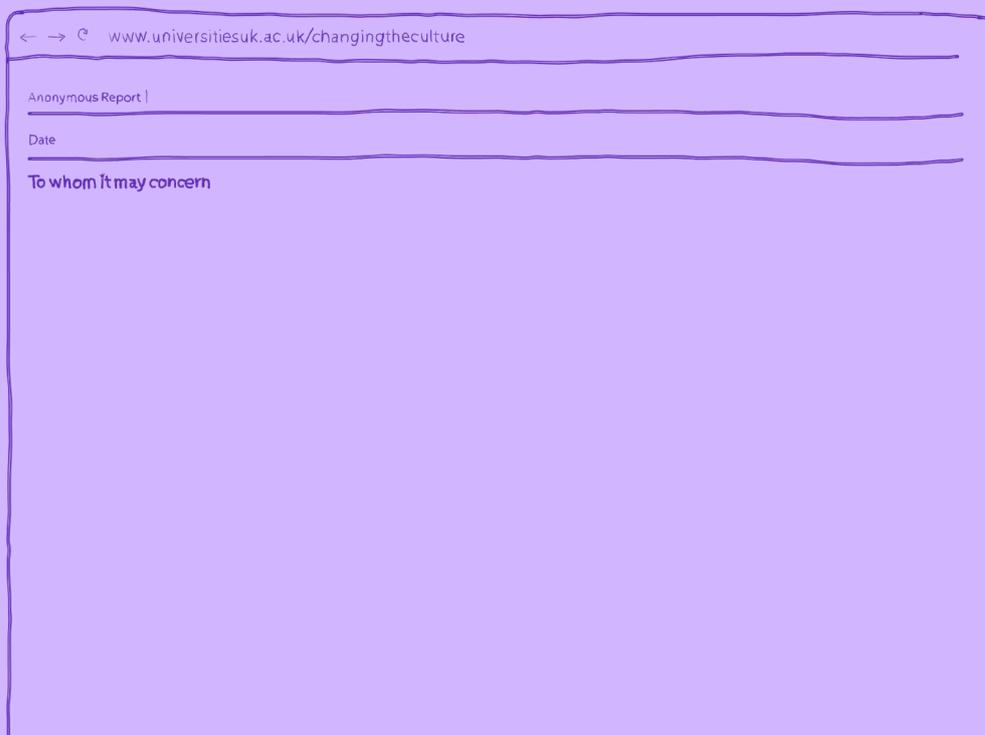
Even if the information to be held is anonymous, **it is still necessary, as part of the obligations and principles relating to transparency in the data protection legislation, to notify individuals that their personal data will be anonymised and used in this way. Universities should update their privacy notices to reflect this.**

Universities should also note that anonymous records could be subject to the **Freedom of Information Act 2000** (FOIA) and may need to be published in respect of any FOIA requests (subject to any applicable exemptions).

Any information that could identify living individuals is not truly anonymised and is considered personal data. In this case, the university would need to establish a lawful basis for holding such data under Article 6 of the UK GDPR (see Annexe 2 of the Practical guide).

# 4.

## Next steps



A hand-drawn illustration of a browser window. The address bar shows the URL [www.universitiesuk.ac.uk/changingtheculture](http://www.universitiesuk.ac.uk/changingtheculture). Below the address bar, there are three input fields with labels: "Anonymous Report |", "Date", and "To whom it may concern". The form is drawn with simple lines and has a light blue background.

< → [www.universitiesuk.ac.uk/changingtheculture](http://www.universitiesuk.ac.uk/changingtheculture)

Anonymous Report |

Date

To whom it may concern

To support implementation of the guidance, universities are encouraged to follow up on the actions below and refer to the **Data Sharing Impact and Risk Assessment** in the **Practical guide**.

### **Update privacy notices and other policies**

- Update privacy notices to reflect that personal data, particularly in relation to outcomes and sanctions, may be shared in certain circumstances relating to harassment cases, disciplinary proceedings and/or complaints, in accordance with data protection legislation.
- Update privacy notices to reflect that reports of harassment may be anonymised and kept for reporting and statistical purposes.
- Update other relevant policies to ensure that these reflect how and when personal data might be shared in connection with harassment cases, or other proceedings or complaints.

### **Training and awareness**

- Ensure that staff who make decisions as to whether to share personal data in harassment cases are aware of how to use the guidance and feel empowered to make informed, pragmatic and considered decisions as to when personal data might be shared, depending on the circumstances of the case.
- Ensure that staff involved in deciding whether to share personal data in harassment cases receive appropriate training in data protection law, and in how to make and document such decisions.
- Ensure that staff who handle harassment cases are able to explain to the individuals involved how their personal data might be shared and what information might be shared with them, to manage expectations.

### **Keep individuals informed**

- Ensure that individuals involved in any harassment cases are kept informed throughout as to when their personal data might be shared and what information might be shared with them, to manage expectations.

Having worked across the sector to prepare the guidance, UUK's view is that the guidance alone cannot address all the challenges regarding whether to share personal data, as there may still be hesitancy in making decisions to share. Universities will need to decide how best to implement the guidance and to instil culture changes that discourage blanket policies not to share personal data.

**The guidance cannot provide definite answers as to what a decision should be in a specific case; this rests with the university in line with its own governance process and the facts of the case.**

**We do, however, hope that by highlighting the clear benefits of sharing outcomes, and where possible sanctions, with reporting parties and by providing a framework to aid universities in their decision-making process, that this will assist staff within universities to take more case appropriate decisions to share personal data while complying with current data protection legislation.**

Over the 12 months following publication of the guidance, universities are invited to share their experiences of how it has been used and implemented, including examples of where universities have used the guidance to take more pragmatic and appropriate decisions to share personal data. In 2023, UUK will hold a full review with a view to publishing examples of how the guidance has been implemented.

Recognising that this is a 'living' document, the guidance is a '**first edition**' and will be updated as feedback on implementation emerges.

Over time, we hope the guidance will support **a shift in institutional culture**, resulting in more transparency in how harassment cases are handled and the sharing of personal data where it is legally appropriate to do so. **By doing this we hope victims-survivors will be encouraged to come forward to make reports.**

## Acknowledgements

The guidance has been prepared and written by Elizabeth Dunford, Principal Solicitor (Technology/Data Protection) at Coventry University, with assistance from members of a Wider Stakeholder Group. Universities UK extends specific thanks to Elizabeth Dunford and the support provided by the Group.

### Wider Stakeholder Group and Advisory Group

- Professor David Richardson, Vice-Chancellor, University of East Anglia, Chair, UUK's Wider Stakeholder Group
- Sarah d'Ambrumenil, Head of the Office of Student Conduct, Complaints and Appeals, University of Cambridge
- Dr Anna Bull, Co-founder, The 1752 Group and Lecturer in Education and Social Justice, University of York
- Nicola Bradfield, Group Director of Legal Services, Coventry University
- Elizabeth Dunford, Principal Solicitor (Technology/Data Protection), Coventry University
- Clarissa Humphreys, Sexual Misconduct Prevention and Response Manager, Durham University
- Refel Ismail, Senior Legal Counsel, London School of Economics and Political Science
- Jenny Jenkin, Secretary and Registrar, London School of Hygiene and Tropical Medical, University of London
- Jill Leigh, Academic Registrar and Head of Institution, The Conservatoire for Dance and Drama
- Gemma McCall, Co-founder and Chief Executive Officer, Culture Shift
- Alison McGrand, Senior Employment Policy Adviser, UCEA
- Helen McNeely, Head of Student and Academic Affairs, Queen's University, Belfast
- Jo Nuckley, Head of Outreach and Insight, Office for the Independent Adjudicator in Higher Education
- Dr Veronica O'Halloran, former University Secretary & Compliance Officer, University of Strathclyde
- Benjamin Parsons, Head of Engagement, AMOSSHE

- Kelly Prince, Independent Researcher, and former Serious Incident Case Officer in Higher Education
- Ben Rogers, Director of Registry Services, Cardiff Metropolitan University
- Helen Scott, Executive Director, Universities HR
- Anne Taylor, Associate Director, Funding Operations and Governance, The Wellcome Trust
- Sean Weaver, Data Protection Officer, Cardiff Metropolitan University
- Angellique Woolery, Operations Manager, GuildHE

We are also grateful for the feedback and input from members of the Information Commissioner's Office, The Equality and Human Rights Commission, Alexandra Potts, Data Protection and Freedom of Information Officer, University College London and Scottish Higher Education Information Practitioners Group.

## Annexe 1: Glossary

<b>complaint</b>	This refers to the complaint raised by the reporting party about the responding party through the university's relevant processes (for example, through the grievance process for employees, or the student complaints process for students)
<b>criminal convictions</b>	Personal data relating to criminal convictions and offences
<b>data protection legislation</b>	The applicable legislation in the UK that governs the processing, sharing, protection and handling of personal data, namely the UK retained version of General Data Protection Regulation (EU) 2016/679 (the <b>UK GDPR</b> ) (as defined in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018) and the Data Protection Act 2018 (the <b>DPA 2018</b> )
<b>data sharing impact and risk assessment</b>	The tool proposed by the guidance and outlined in the Practical guide to support universities in deciding whether it is necessary and justifiable to share personal data in harassment cases
<b>data subjects</b>	An identified or identifiable natural person to whom the personal data in question relates
<b>disciplinary process</b>	A university's internal process for dealing with student and staff behaviour where this breaches university policy or otherwise constitutes misconduct
<b>DPIA</b>	A Data Protection Impact Assessment, as required under Article 35 of the UK GDPR
<b>DSAR</b>	A Data Subject Access Request made pursuant to Article 15 of the UK GDPR

<b>harassment</b>	<p>As defined in Section 26 of the EA 2010:</p> <ul style="list-style-type: none"> <li>i unwanted conduct relating to a protected characteristic under the EA 2010 (being age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership, and pregnancy and maternity) having the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them</li> <li>ii unwanted conduct of a sexual nature having the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them</li> <li>iii unwanted conduct of a sexual nature relating to gender reassignment or sex having the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them and because of the individual's rejection or submission to the conduct, they are treated less favourably</li> </ul>
<b>ICO</b>	<p>The Information Commissioner's Office, the UK's independent authority set up to uphold information rights in the public interests, promoting openness by public bodies and data privacy for individuals</p>
<b>lawful basis</b>	<p>A lawful reason why a university is permitted to process, share or otherwise handle personal data under the data protection legislation as outlined in Article 6 of the UK GDPR (and Article 9 of the UK GDPR in respect of special categories of personal data)</p>
<b>natural justice</b>	<p>The general rule against bias and the right to a fair hearing</p>
<b>NIPSO</b>	<p>The Northern Ireland Public Services Ombudsman, the independent complaints scheme for people raising complaints about public service organisations in Northern Ireland</p>

<b>OIA</b>	The Office of the Independent Adjudicator, the independent student complaints scheme for England and Wales
<b>outcome</b>	Refers to the outcome of the relevant grievance, complaint or disciplinary process (for example, that a complaint or grievance has been upheld, that appropriate action has been taken, or that a responding party will no longer be on campus). This is different and distinct to a sanction
<b>personal data</b>	Any information that relates to an identified or identifiable living individual, as defined in Article 4(1) of the UK GDPR
<b>principles</b>	The overriding principles for the processing of personal data, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability, as set out in Article 5 of the UK GDPR
<b>processing</b>	Any operation or set of operations performed on personal data, including the collecting, holding and sharing of personal data, as defined in Article 4 of the UK GDPR
<b>reporting party</b>	The person who has reported that they have experienced harassment. There will be occasions when a third party such as another student, student representative, staff member or an external party may witness or otherwise becomes aware of an incident and makes a report to the university, in which case the reporting party would be the individual who has experienced the harassment, rather than the individual who in fact reported it.
<b>responding party</b>	The person who has a complaint made against them
<b>sanction</b>	The sanction imposed on a responding party as a result of a disciplinary process (for example, warning, dismissal, expulsion)

<b>sharing</b>	The sharing of personal data between the university and another individual (for example, the reporting party or the responding party) or third party
<b>special categories of personal data</b>	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, or concerning health or a natural person's sex life or sexual orientation, as defined in Article 9 of the UK GDPR
<b>SPSO</b>	The Scottish Public Services Ombudsman, the independent complaints scheme for people raising complaints about public service organisations in Scotland
<b>third parties</b>	Other entities with whom universities may, if a lawful basis is established, share personal data including the OIA/NIPSO/SPSO, law enforcement bodies such as the police, and other institutions
<b>wider regulatory framework</b>	The wider regulatory framework to which universities are subject
<b>witness</b>	A witness to the incident of, or the facts surrounding, the alleged harassment reported by the reporting party, who may be required to give evidence as part of any investigation into such incident either supporting the reporting party or responding party's turn of events.

## Annexe 2: References

- ACAS (2019) Conducting Workplace Investigations
- ACAS (2020) Discipline and Grievances 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) Changing 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.



Woburn House  
20 Tavistock Square  
London, WC1H 9HQ

☎ +44 (0)20 7419 4111

✉ [info@universitiesuk.ac.uk](mailto:info@universitiesuk.ac.uk)

🖱 [universitiesuk.ac.uk](http://universitiesuk.ac.uk)

🐦 [@UniversitiesUK](https://twitter.com/UniversitiesUK)



May 2022  
ISBN: xxxx