office of the independent adjudicator

SUPPLYING PERSONAL DATA TO THE OIA

www.oiahe.org.uk

@oiahe

Effective 25 May 2018

Contents

Contents

Introduction

This document is for higher education providers which supply personal data to the OIA.

Where personal data is shared, the OIA and the provider are acting independently as Data Controllers. The OIA does not act as a data processor 'on behalf of' providers. Nor do providers process personal data 'on behalf of' the OIA. Accordingly, we are not required to arrange individual data sharing agreements or contracts between the OIA and providers. This document is intended to help providers to meet their obligations to document how the personal data they supply to the OIA is used, and to provide assurance that personal data may be lawfully supplied to the OIA.

We take our responsibilities towards personal data very seriously. We always try to operate in accordance with relevant Data Protection Legislation (including the General Data Protection Regulations ('GDPR'), the Data Protection Act 1998 and any subsequent legislation which repeals or amends these.

This document sets out the OIA's understanding of existing guidance, and is specific to our organisation. It does not constitute legal advice. If anything in this document conflicts with guidance issued by the Information Commissioner's Office, that guidance should take precedence.

This document is reviewed regularly and will be updated to reflect any relevant changes in practice at the OIA, as our processes evolve in accordance with good practice guidance.

As an organisation with less than 250 employees, the OIA is not obliged to appoint a Data Protection Officer.

If you have any queries about this document, please contact enquiries@oiahe.org.uk.

21 May 2018

What personal data do providers supply to the OIA?

Providers may supply the OIA with personal data about many different individuals, and the level of detail and type of data will vary.

Staff handling complaints/appeals

All providers will supply the OIA with the name and contact details of a designated 'Point of Contact' ('POC'). We use this information to keep our members informed about the work of the OIA in general (for example, by sending e-news letters) and to send correspondence specific to the provider (for example, invoicing information).

Some providers will supply the OIA with the name and contact details of other members of staff to act as a delegate for the POC.

We keep the contact information about POCs and POC delegates for as long as the person is acting in that capacity. Providers can amend these details at any time via MyOIA our online case tracking system.

We ask that all providers ensure that their POC or POC delegate are based in the UK. Some complaints to the OIA may involve students based at campuses overseas. In these cases, the OIA will share information with the provider within the UK. The provider is responsible for ensuring that disclosure of any data to another country for the purpose of responding to the complaint, is compliant with data protection legislation.

Some providers will also supply the OIA with the name and contact details of other members of staff to enable them to participate in OIA events, for example webinars or workshops. We use this information for administration of the event, and to keep track of which providers have participated in events.

Some providers may supply additional information about staff members to enable the OIA to ensure they can access our events (for example, information about reasonable adjustments required, or dietary requirements). We only use this information for the administration of the event and we will delete it after the event has taken place.

Personal Data in 'Complaint Files'

When we receive a complaint about a provider, we will usually ask the provider to send us its response to the complaint, and we may ask it to include specific information about how the matter has been handled within its own relevant internal procedures. (In some cases, we may not seek any response from the provider; this might happen if we are able to establish quickly that the complaint is not eligible for review by the OIA). In this document, for convenience, we refer to the information sent to us by the provider as 'complaint information' and to all the information we hold about a complaint as our 'complaint file'. Our complaint file will include information supplied by the student, as well as the complaint information from the provider.

Personal data of the student making the complaint

Information which the OIA needs from a provider about a complaint will always include the personal data of the student making the complaint to the OIA. The nature of the information will vary according to the nature of the complaint. It will always include details of the student's name, course of study, and the reason for their dissatisfaction. It may include information about the student's academic progress, and details of activities which they have undertaken as a student. It may include details about the student's residence. It may include details about the behaviour of the student. Some of the personal data may fall within the special categories of personal data, including information about the student's physical and mental health. In a minority of cases, it may include information about criminal offences or alleged criminal offences. The information the OIA needs to review a complaint may also include other information which people commonly expect to be treated with a high degree of sensitivity and confidentiality, including information about race, ethnicity, religion, nationality, gender, sexual orientation, and sexual activity. The personal data about the student may include both verifiable facts, and opinions.

Personal data of the provider's employees

The information we need is also likely to include personal data about employees of the provider, acting in their professional capacity. For example, this will include the names and job titles of members of staff who participated in reaching the decision which the student is unhappy about. It may include information about which elements of a course of study a particular member of staff has responsibility for, or information about a research project which a member of staff is involved in. It may include information about the behaviour of a member of staff. Some of the personal data about members of staff may fall within the special categories of personal data, or include other information which people commonly expect to be treated with a high degree of sensitivity and confidentiality.

For example, a complaint about cancelled classes may relate to the ill-health of a member of staff. A request for additional time to respond to the OIA might include reference to a member of staff being unwell. A complaint about sexual harassment might include information about the sexual orientation of a member of staff. This personal data may be verifiable facts, or may be an opinion.

Personal data of other students

The information we need in order to review the complaint may include personal data of other students. For example, if another student has acted as a witness in a disciplinary matter, we are likely to need to see the statement they gave. Some of the personal data about other students may fall within the special categories of personal data or include other information which people commonly expect to be treated with a high degree of confidentiality and sensitivity. For example, if Student A complains to the OIA that they are unhappy with the provider's response to a complaint about Student B's behaviour, there may be information about how Student B has behaved and any defence Student B presented. Information about other students may be verifiable facts, or opinions.

Personal data of other individuals

It is possible that the provider's records of how the student's complaint was handled under its own internal procedures may include personal data of other individuals, which may be verifiable facts or opinions. This may include information that falls within the special categories of personal data or include other information which people commonly expect to be treated with a high degree of confidentiality and sensitivity. For example, a student might include details of a parent's ill health or a spouse's criminal convictions for violent behaviour as part of their claim for mitigation in an assessment.

The OIA's basis for lawful processing

In order to process personal data in complaint files lawfully, the OIA relies on Article 6 (1) (e) of the GDPR: *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*.

The OIA is the designated operator of the student complaints scheme established under the Higher Education Act 2004. This gives us official authority to operate a scheme for the review of student complaints.

We do not rely upon consent as the "lawful basis" for processing the personal data in our complaint files (Article 6 (1) (a): *the data subject has given consent to the processing of his or her personal data for one or more specific purposes)*. We use our complaint form to notify students that we will process their personal data, highlighting that this may include some sensitive or special category data, and setting out that we will disclose the information they supply to the provider(s) complained about. We also direct them to further information about data protection on our website.

We ask the student complaining to indicate on our complaint form that they have read and understood what we will do with their personal data.

We respect the rights of students to be informed about the use of their personal data, and to object to how it is being processed. Although we do not rely on the student's consent as the lawful basis for processing, we ask students to indicate agreement to us processing their personal data on the complaint form. We also explain that the student may ask us not to process some of their data, or to stop processing all of their personal data.

If it is possible to review a complaint fairly without access to some personal data, we will do so. If it is not possible to review the complaint fairly without access to some personal data but the student objects to that processing, we will explain to the student that we are unable to continue with our review.

Special Category data

We may process Special Category personal data in reviewing a student complaint (including information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, or sexual orientation).

We rely upon Article 9 (2) (g): *Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject*.

The charitable purpose of the OIA is the advancement of education through the independent, impartial and transparent review of unresolved student complaints and the active promotion of good practice in preventing and handling complaints. It is in the public interest that students are able to seek an independent review of their complaints, and that the entire higher education sector should benefit from the learning derived from those reviews.

In some circumstances, we may also rely upon Article 9 (2) (e): *Processing relates to personal data which are manifestly made public by the data subject*.

Lawful basis for providers to disclose personal data to the OIA

The Higher Education Act 2004, defines those organisations which are required to be a member of the OIA Scheme. Section 15 of that Act requires members of the OIA to comply with obligations imposed by the Scheme. In England, membership of the OIA is also a requirement in order for a provider to be listed on the Register established by the Office for Students.

The way we operate the student complaints scheme is set out in our Rules. Rule 3.4 says, *All members of the OIA must comply with the Rules and their procedures and regulations must be compatible with the Rules.*

The Rules set out the obligations on providers to provide us with the information we need in order to review students' complaints:

We may ask for information from the student and/or the higher education provider to help us decide whether we can review the complaint (Rule 10.4)

We may ask the student and/or the higher education provider to answer specific questions and/or provide additional information or documents (Rule 12.2)

The student and the higher education provider must respond to any requests for information we make during our review (Rule 12.4)

If the higher education provider does not provide information requested during the course of our review, or does not provide it within the time limits set, the Independent Adjudicator may report it to the Board, and may publicise it in the Annual Report and/or by other means (Rule 12.6)

We believe that this framework enables providers to rely upon the following provisions to cover the lawful disclosure of personal data to the OIA:

GDPR Article 6 (1) (c): *Processing is necessary for compliance with a legal obligation to which the controller is subject*

GDPR Article 6 (1) (e): *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*

In terms of disclosing special category data to the OIA, we believe that providers can rely upon the same lawful bases provisions as the OIA:

Article 9 (2) (g): *Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.*

and in some cases

Article 9 (2) (e): *Processing relates to personal data which are manifestly made public by the data subject.*

Limiting the personal data dislosed to the OIA

The lawful bases which allow providers to share personal data with the OIA in complaint information, can only be relied upon if the processing is 'necessary'. This means that the OIA and providers must, on a case by case basis, consider what personal data is necessary for the OIA to reach a fair outcome.

As a private individual, the student making the complaint is not expected to abide by data protection legislation. The onus for ensuring that we are processing personal data lawfully rests with the OIA when information is provided by the student. We do not usually make any changes to the way a student chooses to express their complaint to the OIA, before copying this information to the provider. For example, if a student chooses to send us a copy of their thesis, we would include this in the information we send on to the provider, even if the thesis has no bearing on the complaint. However, we may make exceptions to this approach where the student supplies personal data of other individuals that is not necessary for our review, particularly if that information has not previously been disclosed to the provider. When deciding how to approach this personal information we will consider the sensitivity of the information, its relevance to the complaint, and the potential impact on the third party of disclosure. We may redact, anonymise or apply pseudonyms, or we may return personal data to the student if it does not seem relevant to our review.

When information is disclosed from a provider to the OIA, both the provider and the OIA have a responsibility to ensure that the processing is lawful.

We will not request excessive personal data in order to review a complaint. We will not ask the provider to supply 'everything you know about the student'. If a provider receives a request for information which it believes is excessive, it should contact the OIA to discuss this.

However, we usually ask to see all of the information which was considered by the provider in reaching the decision that the student is now complaining to the OIA about. This means that if, for example, a complaints panel received extensive and unredacted personal data about the student, the student's family, members of staff etc, then we may need to see that information to be able to assess the reasonableness of the decision reached by the panel.

To reduce the risk that unnecessary personal data is disclosed to the OIA, providers can take some steps during the internal complaints or appeals process, to manage the amount of personal data being considered. For example, providers may encourage students to limit the amount of personal data they supply about third parties (in particular, in the amount of sensitive personal data about other people's health supplied by a student in support of their claim for mitigation), by issuing guidance about what should and should not be included. Staff carrying out investigations or reviews might be provided with extracts from relevant correspondence or documents rather than full copies.

It may be appropriate for the provider to redact or anonymise information, or use pseudonyms before sending information to the OIA. For example, it would be appropriate to redact Minutes of Exam Boards to remove information about students whose results are considered at the same time as the results of the student complaining to the OIA. It is usually sufficient to remove the students' names completely. However, if it is necessary to refer repeatedly to another individual and to distinguish them from other individuals (e.g. two other students accused of participating in the same incident of misconduct as the student complaining to the OIA) then the names should be removed and replaced by a pseudonym (Student A, Student B, Professor Z etc).

In some cases, it may be appropriate for the provider to use pseudonyms but to also supply the OIA with a key. This will enable us to identify those individuals in the information provided by the student, and be consistent when applying pseudonyms to that information. We will keep the key securely, and where appropriate, the key will be destroyed once the pseudonyms have been applied.

It can also be appropriate for a provider to remove personal data which is not relevant to the complaint before supplying documentation to the OIA. To ensure that the student can be confident in the OIA process, it is important to be transparent and explain that some personal data has been removed.

Informing people that the OIA is processing their personal data

The student

As set out above, our complaint form tells the student complaining to the OIA how we will process their personal data, including exchanging information with the provider. Providers can rely upon the declaration in the OIA Complaint Form as evidence that the student making the complaint is aware that it will disclose their personal data to the OIA. Providers should not need to carry out a separate notification process, or seek consent.

Members of staff / employees

Providers may have an obligation to notify their employees that their personal data is being disclosed to the OIA. The obligation under GDPR to inform a person that their data is being shared is distinct from the lawful bases for processing. Notifying someone that their personal data is being used does not mean that a provider must get consent from every individual referred to in complaint information before answering a request for information from the OIA. The approach which providers take to notifying their employees about this processing may differ according to the level and sensitivity of personal data being supplied:

- Information could be included within the general privacy statement made available to all employees about the possibility of disclosure to the OIA.
- Employees could be reminded during the investigation of a complaint that information gathered during that process could be disclosed to the OIA.
- Specific employees may be explicitly advised that their personal data is being shared with the OIA when the complaint concerns them as an individual in some way. In such cases, the provider could provide the member of staff with a link to the information about data protection which is available on our website and/or to this document.

It may not be necessary to notify the member of staff if the data supplied to the OIA has been anonymised or if a pseudonym has been used. However, thought should be given to the impact of the OIA's transparent process: it is possible that information which is not 'personal data' to the OIA because we are unable to identify a particular member of staff, may become personal data once it is in the student's possession.

Other students

Similarly, the provider may have an obligation to notify other students if their personal data is being supplied to the OIA (and consequently, to the student making the complaint). It may be appropriate to advise all students of this possibility in general terms. It may be appropriate to contact students on an individual basis where it is not possible to anonymise the information being supplied to the OIA, and to direct the student to the information about data protection which is available on our website.

Rights to Object to Processing

When individuals are notified that their personal data is being processed by the OIA, they may wish to object. We will usually be able to take steps to redact, anonymise or otherwise ensure that the person can no longer be identified. Sometimes it is possible to remove the personal data entirely, because it is not relevant to the substance of the complaint. The right to object to processing is not an absolute right to prevent the processing, particularly where an organisation does not rely on consent as the legal basis.

If an individual exercises their right to erasure (the right to be forgotten) in respect of information we have shared with a provider, we will inform the provider. It is good practice for providers to inform us if they are asked to delete personal data which they have previously shared with us.

Individuals have the right to correct personal data which they believe is incorrect. Where the personal data is a matter of opinion, and is itself part of the issue in dispute in the complaint, we will ensure that our complaint file reflects the individual's disagreement with the personal data.

Personal data not directly obtained from the data subject

GDPR Article 14 says that if an organisation obtains personal data from a source other than the data subject themselves, the organisation must tell the person that their data is being processed, why it is being processed, and how it is being processed. This must be done within one month of receipt of the data, and if data is disclosed to another recipient, it should be done at the latest at the point of disclosure.

Organisations do not have to meet these obligations if '*the provision of such information proves impossible or would involve a disproportionate effort... In such case the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests*'. (GDPR Article 14 (5) (b)).

Providers may be given personal data about individuals during a complaint or appeal, usually by the student pursuing the matter but occasionally by members of staff or other sources (e.g. staff at placement providers). In some cases, the provider may already have notified people in broad terms of the possibility that their personal data might be processed. A provider is likely to have contact details for its employees and for its students, but contacting other individuals may prove more difficult.

If a provider does take action to notify a person individually that their personal data is being processed during a complaint or appeal process, it would be helpful to explain that some information could be shared with the OIA.

The OIA receives extensive personal data that is not provided directly by the data subject. In the majority of cases, the OIA does not have any contact details for the individuals concerned. In some circumstances, we may seek assistance from providers to inform these individuals that their personal data is being processed.

In considering whether contacting the person would involve "disproportionate effort" we may consider:

- Do we have contact details for the person? How difficult would it be to obtain contact details?
- Are we able to anonymise the information?
- Do we need to use the information?
- Does the person already know that their information has been given to us?
- Would the person have a reasonable expectation that we would have the information and use it in the way we intend to?
- Is the personal data extensive?
- Is the personal data information which the person has already manifestly made public?
- Is the personal data 'special category' personal data, data relating to criminal offences, or other data which people commonly regard as sensitive?
- Is the personal data about someone acting in their professional capacity?
- Is the processing likely to have any impact on the person? Are we making any decisions about the person? Could the processing cause the person damage or distress?
- Could notifying the person cause them damage or distress?
- Could notifying the person cause another individual damage or distress?

1. A student complains that his supervisor was not suitably qualified to oversee his PhD research. The provider's regulations state that lead supervisors must have a doctorate. The provider sends the OIA a copy of the supervisor's academic CV, confirming that she holds a doctorate. It is unlikely that the OIA would contact the supervisor directly. The personal data is in the public domain.

2. A student supplied medical information relating to her mother in support of an academic appeal. This information is supplied to the OIA by the provider as part of the information it considered at the final stage of its internal processes. The OIA has no means to contact the student's mother directly, but may ask the student to inform her that the personal data is being processed. We will not refer to the personal data in detail or in a way that would identify the mother in our decision.

3. Student A's complaint to the OIA concerns how the provider handled an allegation of sexual assault by Student B. Student A names Student B in the information she sends to the OIA. The OIA anonymises the information. The provider also anonymises the information it sends to the OIA. The OIA does not contact Student B, because the data has been anonymised.

4. Student A's complaint concerns a charge of collusion. He supplies a statement from Student B, admitting that Student A had done the work and that she had copied it in full. This was not what Student B had previously said to the provider. The provider is aware who Student B is. We may ask Student A or the provider to help us contact Student B to explain how their personal data will be used.

What the OIA does with the personal data supplied to us by providers in complaint information

What do we process the complaint information for?

We use the personal data supplied to us by providers in complaint information, to review the individual student complaint we have received. Details of the different kinds of outcome we may reach can be found in our Scheme Rules and accompanying guidance.

In our reviews, we consider the way a provider has responded to a student complaint as an organisation, rather than how individual employees or students or other individuals have acted. Any Recommendations we make are directed towards the provider as a whole, not towards individual members of staff or other students. We make Recommendations about what a provider should do next; we do not take any action directly.

Some complaints may result in a provider deciding to take its own action in respect of its employees or other parties. For example, we might Recommend that a provider re-investigate a claim about bullying. As a result of its investigation, the provider might decide to take action under its staff disciplinary procedures. That is the decision of the provider, not of the OIA.

The circumstances in which the OIA would take any action directly which might affect a person other than the student making the complaint, are extremely limited. It is possible that information obtained by the OIA during the course of a review might indicate that a person has behaved unlawfully, or in a way that raises safeguarding concerns, or in the case of certain professions, behaved in a way which might require further investigation by a professional body. In these limited circumstances, we might refer the information on to the appropriate authorities. In doing so, we would rely upon Article 6 (1) (c) *Compliance is necessary for compliance with a legal obligation to which the controller is subject* and Article 6 (1) (f) *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.*

If, as a result of a complaint to the OIA, we believe that there may be a systemic issue, including systemic safeguarding issues, which would be relevant to the various agencies responsible for quality assurance of higher education courses, and particularly of professionally accredited courses, we may refer the matter to an appropriate body. The referral will not contain any personal data.

We draw upon individual complaints to identify good practice. We use a variety of mechanisms to share good practice, and within this we will use case studies which may be based on a single complaint or may be an amalgamation of several complaints. We may identify providers

in some case studies which we decide to publish in the public interest. We never identify the student making the complaint, or any other individual in these case studies. We ensure that the information we include is not personal data.

We may identify common themes in complaints from a provider and discuss these with the provider. We also carry out analysis of the complaints we receive to identify themes and trends in who complains to the OIA, and what about, across all our membership. Although this may use some of the personal data information we obtain from students and providers, for example, about students' fee status, we do not refer to individuals in discussing trends or themes.

Where is the complaint information stored?

We prefer to receive information from providers electronically. All information received in paper copy is scanned and stored electronically. We operate a clear desk policy. Paper copies of any information related to individual complaints are stored in locked filing cabinets when not in use. When the paper copy is no longer required, it is shredded. We use a specialist confidential waste shredding company to ensure that this information is properly disposed of. Our contract with this company is GDPR compliant.

We store all information which we receive about an individual's complaint in our secure casework database, which is password protected.

While we are carrying out the review, case-handlers may also have an electronic working copy of the documentation, stored in a secure location within our IT systems but outside the database. We do this for reasons of efficiency, so that a case-handler can refer to a single PDF document, rather than cross referencing between multiple attachments on the database. Working documentation is deleted within 6 months after our review has been completed.

Our staff may work remotely, away from our offices in Reading. We provide IT equipment with secure access to the OIA's systems. Staff do not store personal data from complaint files on their own personal devices or systems.

We may receive personal data during telephone discussions with providers and students. All OIA calls (incoming and outbound) are recorded. Usually staff record a written summary of the conversation on the casework database and do not access the audio recording. Audio recordings are stored electronically on a discrete call recording system. Where a conversation is particularly detailed, or becomes the subject of a disagreement, we may store the audio recording within the casework database.

Students may supply their personal data to us via our online complaint form and tracker system MyOIA. Providers may also use MyOIA to supply us with details of POCs and POC delegates.

Who can access the information?

The information may be seen by a number of different staff in case-handling roles at the OIA in order to:

- Log receipt of the information onto our casework database;
- Create a working OIA case file for the decision maker to read;
- Establish whether we need to make reasonable adjustments to our processes for the student;
- Answer enquiries about the progress of the complaint;
- Reach a decision about the complaint;
- Consider the complaint under our quality assurance processes;
- Decide whether further action is required after a complaint has exhausted our processes (responding to requests that we re-open our review or to legal challenges);
- Evaluate the complaint and draw out learning.

Some staff who are not in case-handling roles at the OIA may also access limited elements of the personal data which is supplied to us by providers:

- IT support staff may help case-handlers to access the information in the event of technical difficulties;
- Data analyst staff access our case-handling database in order to carry out statistical analysis of the complaints which the OIA has received.
- Staff with a focus on good practice and sector engagement may access our case-handling database in order to evaluate themes, trends and identify systemic issues.
- Staff responsible for responding to service complaints about the OIA may use personal data in complaint files to inform our response. Service complaints may be escalated to a member of our Board to review.

Who do we share the information with?

We operate a transparent process. Normally, we will send a copy of everything we receive from one party, to the other. This is so that both parties can understand what we have based our decision upon. It is likely that if the provider has carried out its processes in a transparent manner, the student will already have been provided with much of the information during the provider's internal complaints or appeals process.

A student may appoint a representative to act on their behalf, and in those cases we share the information with the representative. If the representative is acting in a professional capacity, it is likely that they will have their own obligations to process the personal data they receive in accordance with data protection legislation.

Either party may submit information to the OIA and ask that it is not shared with the other party. We will consider whether it is possible to share the information in a redacted, anonymised or pseudonymised form. Usually, the OIA will not rely upon information which cannot be shared and will return it to the source. We will explore whether there are compelling reasons not to share the information. Circumstances where we will accept personal data from one party but not share it with the other, are very rare. For example, a student complains that a member of staff at the provider has been harassing him. The member of staff has said that they feel threatened by the student. The student provides evidence of calls received from a particular mobile phone. The provider may supply evidence to the OIA which includes the member of staff's different phone numbers. We may confirm that these numbers are not the same as the number on the student's call log, without disclosing the member of staff's personal phone number to the student.

During the course of our review we may seek advice from our Higher Education Advisory Panel or Disability Experts Panel, or from an external body such as a professional regulatory body. We do not disclose any personal data in seeking this advice.

We may seek legal advice if a decision we have made is or is likely to be subject to legal action. This may involve the sharing of personal data from a complaint file, in a manner which is protected by legal professional privilege.

Can providers and students share the information more widely?

We encourage providers to share our written decisions ('Complaint Outcomes') with relevant staff members and student support services to build upon good practice.

We take steps to minimise the amount of personal data in the Complaint Outcomes we issue. Where possible, we will refer to staff members by job title. Otherwise, staff members, other students and any other third party will usually be referred to under a pseudonym or anonymously. The student making the complaint to the OIA is usually identified. We avoid including detail about sensitive category personal data unless it is necessary to include it to explain the decision we have reached.

It will usually be appropriate for providers to anonymise the Complaint Outcome before sharing it widely. This might include removing details of departments and course names where cohorts of student are small.

We do not place any restrictions on what a student may do with their Complaint Outcome, and they may choose to make it publicly available.

How long do we keep the information for?

During the review process, information is commonly received from providers by email, in hard copy, or via file sharing facilities (e.g. Dropbox). Once the information has been saved into the casework database, local copies are deleted.

All copies of information external to the casework database are destroyed as soon as possible after our processes have been completed in respect of the complaint, and no later than 12 months after our complaint file is closed. Exceptions to this are made where the student has brought judicial review proceedings against the OIA, and may be made where the file format is unusual and cannot be stored within our casework database. In the latter case, we apply the same retention periods to the files held electronically outside the casework database as we apply to the casework database.

Call recordings are usually deleted six months after the date of the call. Audio recordings of conversations which contain significant information relevant to a complaint may be saved into the casework database.

A complete record of each complaint is maintained in our database for two years after the most recent item of correspondence about the complaint. We are implementing a system to remove personal data from our casework database after this time. We will maintain a record of every complaint which we have received, which does not contain any identifying or personal data, for a period of ten years.

An anonymised copy of every Complaint Outcome is kept for a period of six years after it was issued.

Data Security at the OIA

We take appropriate measures to protect the security of the personal information supplied to us by providers.

Security of Premises

Access to the OIA's offices is controlled by an entry management system. Staff gain access to the building and to the OIA's office via an individual access card. The entry management system records the time that any of our access cards are used and this information can be used to investigate security incidents. Access cards do not contain any information that would identify the OIA address in the event that the card was lost.

Visitors must be given entry to the building by a receptionist, and access to the OIA's office by a member of the OIA. Visitors are accompanied throughout their time in the building. No visitors are left unattended in areas where they might gain access to personal data in case files.

Our offices are cleaned by staff employed by a contracted company. Their access to the office can be monitored via the access cards. Our clear desk policy means that they do not have access to personal data in our complaint files.

Access to the building is available between the hours of 6am and 11pm (Monday to Friday); the building is closed at the weekend. The building is covered by CCTV.

IT Security

Our IT systems are appropriately secure and we take robust measures to protect them against cyber attack.

User access control

Our network and physical equipment is password protected with enforced security criteria and regular password changes.

Access to systems is controlled by Active Directory. A user does not have any access to our systems until they have successfully logged in via Active Directory. Active Directory rights are assigned by default to the access requirements of the user's business group. Further access rights are granted or revoked in special circumstances. Users are granted access to systems relevant to their role and are denied access to all other systems.

Software can only be installed by authorised specialists.

Anti-virus

All servers and workstations have anti-virus software installed to protect against malware/ ransomware attacks. The software is updated daily.

All incoming and outgoing email messages are scanned for viruses, phishing attacks, spam and inappropriate content.

Firewalling

The OIA perimeter networks are protected by appliance based firewalls. All workstations and servers have local firewall installed.

Update management

All workstation and server operating systems are updated frequently. All updates are managed centrally.

Backups

Business critical data and systems are backed up hourly to an offsite cloud provider where it is encrypted at rest. Remaining systems are backed up daily and held in a private data centre protected by security measures mentioned above.

Portable equipment

All portable devices are encrypted and equipped with remote-wipe function.

Equipment disposal

Before disposing of IT equipment, we securely wipe data from it and also physically render data storage devices inoperative onsite. All electronic equipment disposal is carried out in compliance with the WEEE Directive 2007.

All staff are expected to take reasonable precautions to prevent access to our systems by unauthorised people. This includes selecting strong passwords and not disclosing them; changing passwords on a regular basis; locking their computer when it is not in use; ensuring access to OIA systems on mobile devices are protected by passwords or fingerprint technology.

When staff cease to work for the OIA, we ensure that all equipment used to access our systems is returned. Staff are not permitted to keep personal records of complaints handled. Access to our IT systems is terminated immediately on the person's last day of employment.

Staff training

All staff receive training on their obligations towards personal data as part of their induction. 'Refresher' training sessions are delivered annually, and are mandatory for staff handling personal data in complaint files. Extensive information and guidance about data protection in relation to complaint files is available to all staff at all times on our intranet.

The OIA is not obliged, as an organisation with less than 250 employees, to appoint a Data Protection Officer. We have a team of people in roles across the OIA who provide advice to colleagues about data protection.

Staff are aware that failure to abide by internal guidance and procedures in respect of personal data may be considered under our Disciplinary process.

Breaches of the OIA's obligations towards personal data

The OIA operates a procedure for any personal data breaches to be reported internally. All such breaches are investigated. We maintain a record of all breaches, and it is used to inform staff training and to drive process improvement. We take action which is proportionate to the breach, which may include contacting a provider if the breach relates to complaint information it has supplied.

We will comply with our obligations under GDPR to report any breach to the Information Commissioner which poses a risk to the rights and freedoms of data subjects.

We ask that if a provider experiences a personal data breach in relation to information supplied by the OIA, such that it is reported to the Information Commissioner, the provider should inform the OIA.

office of the independent adjudicator

'for students in higher education'

Office of the Independent Adjudicator for Higher Education

Second Floor, Abbey Gate
57-75 Kings Road
Reading
Berkshire
RG1 3AB

0118 959 9813

enquiries@oiahe.org.uk

@oiahe

Office of the Independent Adjudicator

Registered Company number: 04823842

Registered Charity Number: 1141289

May 2018