Guidelines for complying with a Subject Access Request

- Most subject access requests are sent to the Data Protection Officer in the first instance, information for the public can be found here [https://www.brighton.ac.uk/foi/requesting-information/index.aspx](https://www.brighton.ac.uk/foi/requesting-information/index.aspx).
- Guidance on SARS for staff can be found at [https://staff.brighton.ac.uk/reg/legal/Pages/SAR.aspx](https://staff.brighton.ac.uk/reg/legal/Pages/SAR.aspx).

The Data Protection Officer will verify and check identification for requests, and will circulate the request to departments of the University.

What follows is guidance for staff on finding, checking and complying with a request.

**Personal Data**

Personal data is any data that directly or indirectly identifies an individual – a data subject (eg a student) has the right to access this information. Whilst we would always try to limit a request, a data subject is within their rights to ask for all personal data held about them. Personal data could be contained within:

- Application forms, database records, photos, access logs, CVs, support records, spreadsheets, paper files, module lists, attendance registers
- The data could be held in university systems – such as SITS or my department/One Drive, or more local systems such as filing cabinets, personal computer drives (storage devices, computer desktops).
- All emails sent and received over the University network are potentially disclosable, see UoB IT Regulations
- As the University is the Data Controller – to comply with a SAR, we also have to consider any data that UoB may have shared with other organisations – this could be for example PSRBs

A student/graduate cannot use the SAR process to obtain official transcripts or certificates (the process for that is documented here [https://www.brighton.ac.uk/alumni/helping-you/index.aspx](https://www.brighton.ac.uk/alumni/helping-you/index.aspx))

1. **Find the information**

It is good practice for one person in each organisational area to coordinate the search for the data – these staff are well placed to know where the data is likely to be, who could have access or copies.

These staff will be identified by the Data Protection Officer and the request sent to those individuals. On receipt of the request the staff member should consider who in their organisational area is likely to have records on the data subject – this could be personal tutors, course leaders, key support staff, line managers— these staff will need to search records for which they are responsible for plus emails, and shared computer drives as well as paper records. This search may extend to personal data on others that is held on personal devices and home PCs if the staff work from home. The search should include all archive data held – including email archives, deleted and sent items still held.
NB - Future developments: The current process for searching documents and emails is that each staff has to do this directly – we will look to running system searches in the future.

Depending on the data subject, other records may exist – if you know that an area of the University could hold records then please let the Data Protection Officer know. Similarly do them know if the data is available directly to the data subject – by logging into student central for example.

In most cases a search of a name or student/staff number will find the data – however some individuals can be identified by a description – ie there is one six foot tall female working in the Vice Chancellors Office – this description identifies Rachel Page despite not using name.

Always check that the data you find in your search relates to the right person – not someone with the same name.

The Data Protection Officer will send an email to servicedesk@brighton.ac.uk if the request includes any data to be retained by Information Services – they will action the request with the respective parts of the department. This search will only include systems owned by Information Services – and not any owned by other departments, or systems where staff or departments add data to core systems – (for example, the search will not include all staff email accounts, departmental sharepoint areas, or one drives).

2. Screening the information

Only information relevant to the request should be released.

- Redact information/metadata which doesn’t add to the response or which if disclosed could potentially compromise the university’s security. Ensure there is no hidden data in the files.
- You should only disclose information which is about the person making the subject access request. Where a document contains personal data about a number of individuals, including the data subject, you should not disclose the information about the third parties.
- If the record is primarily about third parties, withhold it if blanking out is not possible. Contact the third party to obtain consent to disclose the document if possible.
- Take care not to disclose data where a personal description / descriptive data or combination of data could identify another individual
- Relevance – what is relevant or not, will depend on the request. As examples
  - It could be that emails arranging a meeting with the data subject could be withheld, as they are not about them. For the same reason, staff members listed as attending a meeting would not need to be disclosed to as part of a SAR by the staff member – the data is not about them.
  - Lists of students on a course or module – are not about that data subject – but if that list includes assessment marks, progression data then it would need to be disclosed.
- Depending on the request, we wouldn’t necessarily need to disclose data that a data subject already has access to – for example, emails they have directly received. However, if the organization has retained (and therefore continues to ‘process’ them) the data subject may wish to receive these.

Staff data in an organisational context: it is not uncommon for staff data (names, job roles, contact details) to be included with other individuals data – for example as part of their job they may have sent or received information by email, or they may have attended a meeting and are noted in the minutes of a meeting. In most case, we do not need to redact these staff names, however if there is a concern that disclosure will cause undue stress to the data subject or the staff member then staff names should be redacted.
The records may contain correspondence, documents and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity (occupational health reports, GPs, referral documents). In these cases we are required to balance the interests of the third party against the interests of the data subject and often blank out third party information. In some cases we would need to acquire consent from that third party to disclose.

- For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

It is the data that is requested – not the document i.e. a student’s name will appear in many locations across the institution – we are not obliged to disclose every incidence of the name. However if additional records exist against that name then it would need disclosing.

**Screen out duplicate records**

For example, if you have had an email exchange about a person, with colleagues you only need to provide the last email in the exchange if previous correspondence is included within it. In addition you will not need to provide the requester with a copy of that email from each individual copied into the email.

Do take care with data that may be contained in an original email but then the email conversation goes on to be about something (or someone) else – in these cases the requester is only entitled to the original email

**Confidential references**

Do not disclose confidential references written by members of staff to bodies other than the University. However, we do have to disclose references received by the University.

For example, if you give a reference for one of your staff, you do not have to disclose that reference in response to a subject access request. However, if you have received a reference for one of your staff, that reference does not qualify for an automatic exemption.

**Preventing and detecting crime**

Do not disclose information which would prejudice the prevention or detection of a crime.

For example, if the police informed us that a student is under investigation, but the student did not know this, then that information should not be provided to the student whilst the investigation is in progress.

However, if the investigation is closed or if the student has been informed that there is an investigation underway, then the information should be disclosed.

**Legal advice**

Do not disclose any records which contains requests for legal advice or received as part of legal advice from the in-house legal advisor, lawyers acting on behalf of the University.

**Unfavourable information**
You may discover material which does not reflect favourably on the University. For example, you may find documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed. However, you should bring their contents to the attention of the relevant manager, and ensure that appropriate action is taken to address any issues they raise.

You must not destroy or refuse to disclose records because they would be embarrassing to disclose: this is a criminal offence if it is done after you know a subject access request has been made.

3. Redacting documents

- Save the document (or series of combined documents) as a PDF.
- When in Adobe, from the ‘tools’ menu, select ‘redact’ – then select ‘mark for redaction’, and then ‘text and images’, a cursor will allow you to select areas (by dragging your mouse over the selected area whilst holding the right button of the mouse) of your document, redact all areas as required and then select ‘apply’.
- Save the document as a separate copy.

Redacting hard copy documents

- Print out the document or, if it is a paper record, make a photocopy.
- Using a black marker pen, blank out the exempt information.
- Make a photocopy (or scan) of the blanked out version. This is the copy that will go to the person making the request.

4. Sending the document to the Data Protection Officer

Once the documents have been screened and redacted, they need to be shared with the DPO. The DPO will do a final of the documents to ensure no data is shared that should not be, and that no data is missing.

- Paper documents should be delivered by hand where possible.
- Electronic documents need to be shared securely – ideally through an encrypted email, or if there are many documents, place all the documents in a secure One Drive file, or Sharepoint folder – give access to Rachel Page.
- PDF is the preferred format for electronic files.
- Flag any documents you are still concerned about disclosing and have not already had guidance on.
- For technical files, or data exports, you may need to provide a narrative of the data – which would be shared with the requester
- Please inform the Data Protection Officer if any of the data can be accessed directly by the data subject.

All email correspondence should be directed to Rachel Page at dataprotection@brighton.ac.uk – this is a shared inbox and ensures emails are picked up

5. Preparing for Subject Access Requests in the future:

Responding to subject access requests can be lengthy and time consuming process. Below are some tips to help them be more manageable in the future
Staff are encouraged to do a regular ‘clean up’ of their mailbox so that they are not storing long trails of emails.

If an email conversation goes off topic ensure you remove/redact any personal information that may be contained in the original email.

If discussions are had via email regarding what to reply to a student, these conversations can be deleted once the agreed wording is sent.

Delete old emails where you are cc’d (since you are not the main recipient and data may now be inaccurate or superseded)

If you need to discuss a data subject by email - only ever include details of one data subject at a time, do not include unnecessary detail and ensure data is shared only with those authorised to view it.

If there are no consequences from information within an email being unavailable in the future then delete it. For guidance on how long data should be retained for see the Retention Schedules https://staff.brighton.ac.uk/reg/legal/Pages/records.aspx

Avoid circulating documents via email, use links to shared areas instead – this stops multiple versions of the document being duplicated, uses less storage and removes the need for all the duplicates to be weeded out for a Subject Access Request.

If the information (the decision or outcome) is stored elsewhere (e.g. committee notes, SITs/SharePoint) delete it.

If you are seeking general guidance about a situation – do not use identifying data

Store and share data in one location and provide links to it....this way multiple staff don’t have copies of the data in their email inboxes, or will have made local copies/print outs

Take steps to limit the locations where data is stored – if you can access data from a sharepoint file, you don’t need to email to yourself or save a copy on a mobile device.