1. INTRODUCTION

The European Union Data Protection Regulation (GDPR) provides new rights for people whose data we hold and new responsibilities for all members of the University Group. The GDPR came into force on 25 May 2018. At the same time, a new UK Data Protection Act will has been enacted to enable the UK to maintain the same standards of privacy when it leaves the European Union. As the University is a global organisation, the law applies to the personal data we communicate and receive in the course of our activities worldwide. This means that the law applies to research undertaken on all of our UK and international campuses, in academic partnerships and by fieldwork, no matter where in the world these activities take place. This guide for researchers is one of a series of communications for different groups within the University. The changes that affect research are set out in this guide and can be summarised as follows:

- We can no longer rely on consent to process personal data for many research activities
- We need to be transparent and fair to people whose data we process
- All research projects involving personal data need a proportionate Data Protection Impact Assessment as part of the Ethical Approval process
- We need to apply privacy by design to our research projects and data management plans

2. WE NEED A VALID CONDITION FOR PROCESSING PERSONAL DATA

Under the GDPR we need to have a *lawful condition* for processing for each item of personal data we hold. We can’t justify collecting or holding on to personal data “just in case”.

CAN WE USE CONSENT TO PROCESS PERSONAL DATA FOR RESEARCH?

In relation to research, we have to make a distinction between

1. obtaining consent from individuals to *participate* in research projects to meet ethical requirements, and where necessary to comply with the common law duty of confidentiality; and
2. consent as a lawful condition for *processing* their personal data, once their consent to participate has been obtained.
In order to be able to demonstrate compliance with the GDPR, the University can rely on consent as a condition for processing personal data for research purposes only in limited circumstances, where

- We first obtain the data subject’s specific, informed and freely given consent, 
  So, consent must be voluntary and we need to tell them what we will do with their data before they agree that we can use it, 
  AND
- The data subject gives consent, by a statement or a clear affirmative action that we document, 
  So, we must demonstrate that someone has opted in e.g. by ticking a box. If we ask someone over the telephone for their consent, we must keep a record of their consent and send them a confirmatory email or letter. Use of silence, pre-ticked boxes or “unless you opt out we will…” doesn’t provide lawful consent. 
  AND
- The data subject can withdraw their consent at any time without detriment to their interests. It should be as easy for someone to withdraw their consent as it is to give it e.g. by clicking an unsubscribe link in an email 
  So, if the data subject withdrew their consent would we then be able to stop processing their data? If the answer is no: then consent is not valid.

**IS CONSENT THEREFORE A VALID CONDITION OF PROCESSING PERSONAL DATA FOR RESEARCH?**

<table>
<thead>
<tr>
<th>YES</th>
<th>For projects where</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• We obtain the data directly from the research participant</td>
</tr>
<tr>
<td></td>
<td>• The participant can withdraw their consent for us to process their data and ask us to delete it without detriment to the success of the project</td>
</tr>
<tr>
<td></td>
<td>• Where the University does not intend to reuse or allow other parties to reuse the research data</td>
</tr>
<tr>
<td></td>
<td>Example: an undergraduate or postgraduate taught student dissertation e.g. a survey of body image perception or user interactions with a robot</td>
</tr>
</tbody>
</table>

| NO  | For any project where the above conditions do not apply |

**IF CONSENT IS NOT VALID, HOW CAN WE LAWFULLY PROCESS PERSONAL DATA FOR RESEARCH?**

For most research purposes we rely on the following conditions of processing.
GDPR Article 6 gives us a valid condition for processing personal data where this 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”

As the University is a public authority we may process personal data for academic research purposes as this is one of our core objectives under the University Charter. We can also reuse personal data originally obtained for another reason for research purposes where we can demonstrate that this is in the public interest.

### ADDITIONAL CONDITIONS APPLY TO SENSITIVE PERSONAL DATA.

Sensitive personal data is called special categories of data under the GDPR. This includes personal data revealing someone’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; data concerning mental or physical health, sex life or sexual orientation and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person.

In order to process sensitive personal data for research purposes we also need to comply with GDPR article 9 by demonstrating that:

“Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”

AND

We comply with the safeguards set out in Article 89(1) of the GDPR and the provisions that will be set out in the new UK Data Protection Act. These state that the processing must 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 the interests of the data subject.” More information about these safeguards is in section 5 of this guide.

Please note that the public interest does not justify breach of confidence. We can’t use this condition to justify disclosing confidential personal data e.g. patient data, under common law.

### 3. WE NEED TO BE TRANSPARENT IN OUR USE OF PERSONAL DATA

We have to explain clearly to people what we do with their data and why.

### WHERE WE RECEIVE PERSONAL DATA DIRECTLY FROM THE PARTICIPANT

The participant information sheet we give to each person that we recruit e.g. to be interviewed or take part in an online survey, needs to incorporate all of the elements of a privacy notice:

- The name and contact details of the data controller. This may be the research sponsor e.g. for a study on housing need commissioned by the Scottish Government, or the University may be the sole or joint Data Controller in the context of a partnership project.
• Enough information, in clear language, for the participant to understand what the project is about and what is required of them; what you will do with their data and why
• Any significant risks involved
• Safeguards put in place to mitigate those risks
• The legal basis is that we rely on to process their personal data
• Who they can contact for more information (Principal Investigator),
• The contact details of the Data Protection Officer
• What rights participants have as data subjects, including, where processing their data is based on consent, the right to withdraw consent at any time
• The right to complain to the Information Commissioner’s Office (ICO)
• Assurances that their data will be held securely and treated in accordance with their rights
• The planned retention period for data or the rules that govern retention policy
• Consent to participate in the research

In addition, only where relevant:

• If applicable to medical research, consent under the common law duty of confidentiality
• The recipients, or categories of recipients of the personal data
• Whether the data subject has a statutory or contractual obligation to provide the data and the consequences, if any of not providing it
• Where the data is to be used for automated decision making, a clear explanation of the logic of the process and the consequences for the data subject
• If their data is to be transferred outside Europe, the specific safeguards under the GDPR in place to protect their privacy
• Whether their data may be reused for academic research purposes by the University or external higher education, public sector, charitable or commercial organisations

If we are communicating this information online, we can provide some of the information by means of a link to our own, or the sponsor’s privacy notices. If, on the other hand, we are handing out a paper copy of the privacy notice, particularly in a context where the data subject does not readily have internet access, we need to provide all of the information in one document.

WHERE WE RECEIVE THEIR DATA FROM A THIRD PARTY, SUCH AS ANOTHER UNIVERSITY

The Data Controller transferring the data to the University will have its own obligation to inform the data subject that their data will be shared with third parties.

However, unless a specific exemption applies, we also have a duty to provide the data subjects with the information listed above. In addition our privacy notice needs to state

• Where we obtained their data
• What categories of personal data we obtained

We need to provide this information to the data subject within a month of receiving it OR at the latest, at the point that we contact the data subject, if applicable. If we intend to disclose their
data to a third party, e.g. another university for reuse in research, we need to inform the data subjects before disclosing their data.

**WHEN DON’T WE NEED TO PROVIDE A PRIVACY NOTICE TO PEOPLE WHOSE PERSONAL DATA WE HAVE RECEIVED FROM THIRD PARTIES?**

We are exempt from this requirement when the following conditions apply.

<table>
<thead>
<tr>
<th>Technical and organisational measures are in place to apply the principle of data minimisation. In practice, wherever possible this should mean that we have received the data in pseudonymised form and we conduct the research without being able to re-identify the data subjects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
</tr>
<tr>
<td>It is not possible, or would require disproportionate effort, to provide the privacy notice directly to the data subjects. Here, the age of the data and the number of data subjects are also factors to consider.</td>
</tr>
<tr>
<td>OR</td>
</tr>
<tr>
<td>By doing so we would defeat or seriously impair the objectives of the research. Where we believe that providing the privacy notice directly to the data subjects would undermine the research results we are obliged to consider whether an alternative method of analysis could be used instead.</td>
</tr>
</tbody>
</table>

If this exemption applies we must still make the privacy notice public by publishing it on the research project website and/or in Pure.

We also need to explain and document our reasoning in the Data Protection Impact Assessment for the project.

**4. INTEGRATE PRIVACY BY DESIGN INTO RESEARCH PROJECT MANAGEMENT**

Data Protection by design and default is mandatory under GDPR. From the start of each new project or initiative involving the use of personal data, we need to consider the risks to the rights and freedoms of data subjects (e.g. research interviewees) and what actions we need to take to mitigate those risks and comply with the GDPR data protection principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Security
More information about these principles is in our [Data Protection Policy](#). To help colleagues to apply this methodology in a proportional and consistent way, we have developed a new Data Protection by Design workbook. This incorporates all the elements of a Data Protection Impact Assessment.

**EMBED DATA PROTECTION IMPACT ASSESSMENT WITHIN ETHICAL APPROVAL PROCESS**

All research proposals involving human participants or reuse of personal data obtained from the University or third parties will need to undergo a *proportionate* Data Protection Impact Assessment (DPIA) as part of the [ethical approval](#) process conducted by each School's Ethics Committee.

DPIA involves:

<table>
<thead>
<tr>
<th>Describing the proposed data collection storage and management methodology, data flows and the purposes of the processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing the necessity and proportionality of the processing operation in relation to the purposes</td>
</tr>
<tr>
<td>Identifying the risks to the privacy rights of individuals <em>e.g. the loss of a laptop containing transcripts of interviews with participants</em></td>
</tr>
<tr>
<td>Specifying the organisational and technical measures needed to mitigate them and comply with the GDPR <em>e.g. encrypting the laptop</em></td>
</tr>
<tr>
<td>Agreeing actions to apply these measures and embed privacy by design into the Research Data Management Plan for each project.</td>
</tr>
</tbody>
</table>

For routine research activities such as undergraduate projects, a generic DPIA will be used to specify the security controls and other safeguards required to protect the data.

Under GDPR it is now mandatory to carry out a full Data Protection Impact Assessment before embarking on processing that is likely to result in a high risk to the privacy of individual data subjects. Our [Data Protection by Design workbook](#) includes screening questions enabling researchers to identify proposed activities that will need the full DPIA and then sets out the steps to be taken to complete the DPIA. If the research involves processing special categories of personal data the DPIA will have to demonstrate the public interest that justifies processing without consent.

Principal Investigators are responsible for uploading completed DPIAs and [Data Management Plans](#) to Worktribe as part of the approval process for projects involving external funding.

DPIAs also need to be lodged with the School's records of ethical approval.

The DPIA and DMPs need to be kept as part of the essential records for all projects for as long as the research data they refer to is retained. Wherever possible the completed DPIA should be published in Pure along with the project publications and other outputs. Any
5. APPLY SAFEGUARDS TO PROTECT PERSONAL DATA

THE PUBLIC INTEREST TEST

If we wish to process sensitive personal data without consent for research purposes we need to demonstrate that:

1. the processing is necessary in the public interest

For example, it may be necessary to conduct the research to inform policy or measures to reduce inequality or improve public health; or that data gathered for one project may need to be archived so that it can be used in long term longitudinal studies. The processing needs to be proportionate to the objectives of the research.

We need to document the reasons that we consider processing to be in the public interest in our DPIA. This should reference any relevant independent governance framework. Examples include:

- Peer review from a public funding body such as a research council
- Review by a Research Ethical Committee recognised by the UK Research Ethics Committee Authority in line with the Medicines for Human Use (Clinical Trials) Regulations 2004
- Support from the Public Benefit and Privacy Panel for Health and Social Care, for access to NHS patient data in Scotland or the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA) for access to NHS data in England and Wales

2. That the public interest is not outweighed by the adverse impact on the data subject

Therefore, we need to demonstrate that the processing is not:

(a) carried out for the purpose of measures or decisions with respect to a particular data subject; or

(b) likely to cause substantial damage or substantial distress to an individual

The conditions under 2 (a) and (b) above are set out in the UK Data Protection Bill which is being considered by Parliament at the time of writing (April 2018). Any changes incorporated in the final version of the Act will be incorporated in this guide and communicated to Schools and Services. Some of this guidance is based on the [NHS Health Research Authority researcher guidance](#) and will be reviewed and updated as that guidance evolves.
DATA MINIMISATION

Data minimisation is one of the key principles of the GDPR. We need to collect the minimum personal data necessary for the research purpose required and keep it for the minimum length of time.

Whether possible, pseudonymise the personal data by redacting it from the working dataset, replacing an individual’s and other identifying data with one or more unique codes so that a reader can’t identify the individuals concerned. The file containing the link between the codes and the participant identities will need to be encrypted and stored separately on a University system with access strictly limited on a need to see basis.

Better still, can the information be anonymised so that it ceases to be personal data altogether? For example, actuarial studies can use anonymized published statistics.

OTHER TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

As part of the ethical approval process we need to articulate how we are going to apply the security controls and embed these measures in the Research Data Management Plan.

These will include references to the relevant University information governance policies and procedures and where relevant, standards and policies mandated by the funding body.

We already have a simple information security classification system which takes a proportionate approach to protecting personal data and other confidential information at rest, in use and in communication.

GDPR explicitly requires information systems to be resilient so that data can be recovered and access and functionality restored after an incident. This means that we need to use University IT and email systems to process and store research data as these are secure and automatically backed up to ensure their resilience.

Any portable device e.g. laptop, smartphone, tablet, memory stick or external drive temporarily needed to store or process research data, must be encrypted and protected by a strong password. This brings peace of mind and reduces the risk of enforcement action from the Information Commissioner’s Office (ICO) if the device is lost or stolen.

As fieldwork, by definition, takes place off campus, researchers also need to apply the security standards set out in the Mobile Working Policy. [Link to follow]

As most research data is born digital, we need to manage datasets actively to maintain their integrity as evidence and reduce threats caused by technological obsolescence. More information is on our research data management pages and here.
6. COMPLYING WITH THE RIGHTS OF DATA SUBJECTS

Although the GDPR increases the rights of data subjects, important but conditional exemptions apply to personal data processed for research purposes.

When data processing is necessary for research purposes and where we can meet the conditions set out in this section, the University may lawfully be exempt from the need to comply with the following rights of data subjects.

<table>
<thead>
<tr>
<th>Access</th>
<th>Rectification</th>
<th>Erasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restriction</td>
<td>Portability</td>
<td>To object to processing</td>
</tr>
</tbody>
</table>

In order for these exemptions to apply we must be able to:

Apply the necessary safeguards set out in section 5 above to protect the data and privacy of the individuals concerned;

AND

Justify a decision that complying would prevent or seriously impair the achievement of the research purpose. The number of research participants and the timing of the request are factors to be considered. It may be possible to comply with a research participant’s request to cease processing and delete their data at the early stages of a study but not at a later stage without significantly impacting on the research. Resource implications and available technology may also be relevant considerations.

AND EITHER

• The results of the research or any resulting statistics are will not be published in an identifiable form,

OR

• In the opinion of an appropriate health professional, disclosure to the data subject is likely to cause serious harm.

The law requires us to respond to people’s requests about their own personal data (data subject requests) free of change within one month. This applies even if our response is to refuse the request. If you receive a data subject request for personal information gathered in the course of research please ask HIG@hw.ac.uk for advice straight away.

7. COLLABORATIVE RESEARCH

Where a research project involves working in partnership with other organisations, it is necessary to establish whether the lead organisation is the Data Controller and the others
Data Processors or whether each partner is jointly a Data Controller for the personal data processed in the course of the project.

Each party will need to sign up to the relevant data processor or data sharing agreement as well as the overarching collaborative agreement. Legal Services and the Information Governance team are on hand to advise and provide the agreement templates.

Visiting Scholars, such as academics and students, emeritus professors or honorary fellows who need access to University IT facilities or personal data to conduct research are subject to the same policies and procedures as University staff and students, such as the IT and Communications Facilities Acceptable Use Policy. The Head of School or Principal Investigator is responsible for ensuring that Visiting Scholars sign up to a confidentiality agreement, receive a verbal and written briefing on the information security standards that apply to the project and, where appropriate, complete our online training.

8. PUBLICATION, REUSE AND RETENTION OF RESEARCH DATA

**PUBLICATION OF RESEARCH DATA CONTAINING PERSONAL INFORMATION**

Pure, the University’s research information system, can be used to publish research data as well as papers and other publications. Where papers or underpinning data contain personal data, one of the following conditions will need to be met to enable lawful publication.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>The University has the individual’s consent to publish information that</td>
<td>The University has the individual’s consent to publish information that</td>
</tr>
<tr>
<td>would identify them directly or indirectly. Consider the degree of risk</td>
<td>would identify them directly or indirectly. Consider the degree of risk</td>
</tr>
<tr>
<td>that the person might subsequently withdraw their consent and how you</td>
<td>that the person might subsequently withdraw their consent and how you</td>
</tr>
<tr>
<td>would comply with their “right to be forgotten”.</td>
<td>would comply with their “right to be forgotten”.</td>
</tr>
<tr>
<td>The data is pseudonymised so that it is not possible to identify the</td>
<td>The data is pseudonymised so that it is not possible to identify the</td>
</tr>
<tr>
<td>individual directly or indirectly from the information published about</td>
<td>individual directly or indirectly from the information published about</td>
</tr>
<tr>
<td>them.</td>
<td>them.</td>
</tr>
<tr>
<td>The data is completely anonymised, so that it is no longer personal data</td>
<td>The data is completely anonymised, so that it is no longer personal data</td>
</tr>
<tr>
<td>e.g. statistics.</td>
<td>e.g. statistics.</td>
</tr>
<tr>
<td>The individual has already made the data public e.g. by giving a TV</td>
<td>The individual has already made the data public e.g. by giving a TV</td>
</tr>
<tr>
<td>interview or the data is otherwise already in the public domain e.g.</td>
<td>interview or the data is otherwise already in the public domain e.g.</td>
</tr>
<tr>
<td>a published court judgement.</td>
<td>a published court judgement.</td>
</tr>
</tbody>
</table>

**RESEARCH, PUBLIC ENGAGEMENT AND CHILDREN**

Personal data about children under 16 is subject to specific protection under the GDPR. While under UK law a child of 13 or above is considered to have sufficient maturity to consent to the processing of their personal data, consent from a parent or guardian may still be required to participate in research or public engagement. In the University context the most likely area of impact is in relation to public engagement activity involving children, such as science festivals or workshops in schools, where images and recordings may be made to demonstrate impact and for promotional purposes. In these situations we need to obtain the informed consent of the participants, at least verbally, to publish their images online. This is particularly important when photographing individuals and small groups of potentially identifiable people. To record more general crowd scenes of a venue or a speaker addressing an audience it is sufficient to
put up prominent notices making it clear that filming and photography will take place for promotional purposes. We also need to provide information in a form that participants can take away e.g. a postcard with contact details to find out more about the University or the initiative e.g. Year of the Sea, with a link to the relevant privacy page on our website.

When collecting and using children’s personal data we have a particular obligation to provide this information using “clear and plain language that the child can easily understand.”

We also need to be aware that when a child reaches 18 years of age, they have the absolute right to require the University to take down any images of them posted online. In a situation where a child’s personal data has been shared with another organisation, for instance published online on a University social media account in a post which is then shared on other social media accounts, and the individual asks for their data to be erased, the University must take reasonable steps to inform the other account holders and service providers of the data subject’s request and tell them to erase any links to, or copies of, their personal data.

**REUSE OF RESEARCH DATA**

The Research Council [common principles on data policy](#) state that

“Publicly funded research data are a public good, produced in the public interest, which should be made openly available with as few restrictions as possible in a timely and responsible manner.”

UK Research and Innovation recognises that legal and ethical constraints apply to the release of personal data and requires researchers to consider and address these issues in the data management plans and at all stages of a project.

**What if data can’t be anonymised or pseudonymised for reuse?**

If it is not feasible to anonymise or pseudonymise personal data for reuse we would need to apply stringent safeguards before it can be reused. These datasets will need to be stored in the University research data repository, rather than in Pure. Any research proposal or request from a researcher for access to the data would need to be approved by the relevant School research ethics committee who will review the original ethical approval application, DPIA and data management plan. If the purpose of the new research is sufficiently different from that of the original or would present new risks to the data subjects, a new DPIA will be required. Where the participant information sheet previously issued to data subjects would not have given them a reasonable expectation that their data would be reused in another project we would also need to inform them before reusing their data or sharing it for reuse by an external organisation or researcher.

However, the same exemptions to the requirement to inform data subjects set out in the Transparency section (3) of this guide apply in this context too.
Any personal data disclosed to or received from third parties must be subject to the University’s Data Sharing or Data Processor Agreements, or the funder’s agreement where we apply to receive data from elsewhere.

These data-sharing agreements will prohibit

(a) use of the released data to identify participants or otherwise breach confidentiality

(b) unapproved contact with participants

Please contact RES or HIG for more advice.

**APPLYING RECORDSRETENTION POLICIES**

Our [Research Data Management Policy](#) requires us to retain research data to enable appropriate access and use, for as long as required to meet funders’ requirements.

Research Data that is deemed to be worthy of permanent preservation shall be transferred to or the University archival repository or the appropriate repository designated by the relevant Funder. Information Services can advise on storage.

For advice about records retention please contact HIG at the address given below. You can find more detailed records retention policies for each academic and professional service function on our web pages here. [https://www.hw.ac.uk/services/heritage-information-governance/manage/what-to-keep.htm](https://www.hw.ac.uk/services/heritage-information-governance/manage/what-to-keep.htm)

**9. MORE HELP AND ADVICE**

We’re here to help. If you have a question about any aspect of this guidance please contact:

<table>
<thead>
<tr>
<th>Research Enterprise Services</th>
<th>Information Governance</th>
</tr>
</thead>
</table>
| RES Research Development Team and Legal Services  
res.research@hw.ac.uk  
Advice on developing, constructing and costing research proposals and contracts | Infogov@hw.ac.uk  
Data Protection Officer and Information Governance team  
+44 (0)131 451 3218/9/3274 |

<table>
<thead>
<tr>
<th>Information Services</th>
<th>EBS Research</th>
</tr>
</thead>
</table>
| IThelp@hw.ac.uk  
Advice on data storage, costing research data, data security  
open.researchdata@hw.ac.uk  
Advice on data management plans and use of Pure | Stewart.Smith@ebs.hw.ac.uk  
Stewart Smith, Compliance Manager  
+44 (0)131 451 4764 |