Data protection checklist: Teaching, research, knowledge transfer, consultancy and related activities

All activities which involve personal data of any kind, in any way, must comply with data protection legislation (the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA)). This checklist outlines the requirements of the data protection legislation and the measures you must take when processing personal data; it also provides a mechanism for recording the steps you will take to ensure the personal data you are using are safeguarded and the reputation of the University is upheld.

Ensuring personal data are processed transparently, fairly and lawfully with due regard for individuals' privacy and ensuring that personal data remain secure are paramount. Demonstrating that we have considered the requirements of data protection legislation when conducting our activities will provide assurances to students, employees, research participants and business partners that their personal data is protected at UCLan. Organisations can be fined up to €20 million or 4% of global annual turnover for breaches of the GDPR; therefore it is important that we get it right from the outset. If it is possible to use anonymised data so that individuals cannot be identified from it and still achieve your aims, this is always the preferred method of operating. Truly anonymised data (which cannot be reconstructed or linked to any other data you hold or may hold in the future to enable you to identify individuals from it) does not constitute personal data because it cannot be used to identify individuals.

Section 1: Does my activity involve personal data?

What is *personal data*?

Personal data is data relating to a living individual who can be identified from those data (or from those data and other information in our possession or likely to come into our possession).

Personal data can be factual (such as name, address, date of birth) or can be an opinion (such as a professional opinion as to the causes of an individual's behavioural problems or a response to a survey question). Voice recordings are personal data because the individual can be identified from his or her voice. Information can be personal data even if it does not include a person's name or other obvious identifiers. ***Example***: *a paragraph describing a specific event involving an individual or a set of characteristics relating to a particular individual may not include their name but would clearly identify them from the set of circumstances or characteristics being described or represented.*

If you are unsure whether or not your activity involves personal data, please contact the Information Governance team to discuss on DPFOIA@uclan.ac.uk.

More information about personal data is available in the Data Protection Policy.

What is *processing*?

The GDPR is concerned with the processing of personal data. 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Does your project involve personal data?	Yes	*Opinions obtained during the interview regarding the research topic.*
If yes, are you processing that data? If you have any kind of access to that data, including just holding it, you are likely to be processing it.	Yes	*Interview transcripts will be processed for the final write-up of the thesis.*

If your proposed activity involves processing personal data, you must complete the remainder of this checklist, providing answers to each relevant question.

Section 2: Have I addressed all the key areas of data protection compliance?

This checklist will ensure that you have properly considered how you are processing the personal data you are collecting. You should be able to answer 'yes' to all questions or explain why the question is not applicable. You must provide details to support your answers so that your proposal can be approved. If you are a researcher completing this form as part of your ethics application, you can complete parts of this checklist by referencing your answers on the relevant parts of your Ethics Application Form, if they cover the same detail.

Type of activity:	Interview recording and transcription
Activity name/ title:	**Religious Freedom & State Recognition of Belief**

Processing personal data transparently, fairly and lawfully

Data protection legislation requires us to process personal data transparently, fairly and lawfully. In practice, it means that you must:

- have lawful grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate *privacy notices* when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and make sure you do not do anything unlawful with the data.

1. **Have you checked and confirmed that the intended uses of personal data (including special category data or criminal convictions data) have a lawful basis?**	Yes	*List of personal data included:* *– name of the participant* *– organisational/institutional email address* *– role in the organisation/institution*
2. What is the lawful basis for processing the personal data? *In almost all cases at UCLan, the lawful basis for processing personal data for research purposes will be that the processing is necessary for a task carried out in the public interest (Article 6(1)(e) GDPR). If you think there is an exceptional reason why this does not apply to your research, there are alternative lawful bases from the GDPR which can be considered. You must contact the Information Governance team for advice, particularly if you are considering relying on consent as a lawful basis. Further information about lawful bases can be found here.*		*A task carried out in the public interest.*
3. Are you processing special category data or criminal convictions data?	Yes	

4. If the answer to question 3 is 'yes', what is the lawful basis for processing this type of personal data? *If you are processing this type of data for research purposes and the processing is in the public interest, the lawful basis is likely to be Article 9(2)(j) GDPR by virtue of section 10 and Schedule 1(4) DPA.*		• *I will be processing information regarding opinions about religion, specifically religious freedom, but crucially, not the religious beliefs of participants. To confirm, the religious beliefs of participants will not be part of the questions asked of them.* • *I will ensure that the organisational affiliations of participant are in the public domain already because this is important in conveying their expertise.*
5. **If the intended use of the personal data would or would be likely to have an adverse effect on one or more individuals, have you considered and documented why that adverse effect is justified?**	Not applicable	*I will take care to the best of my ability that the content is plain and factual, thus providing credible references for each statement made so as to reduce the chances of manipulation. I will be reporting on facts and wherever I report on opinions, these will be experts in the field.* *Some negative implications of the study may include:* • *The sanctioning or further sanctioning of expert participants; this type of event was witnessed recent with regards to the Chinese government sanctions on several USCIRF commissioners.* • *I, myself, as the author of this research may experience my own sanctions as a result of the publication of this thesis such as travel bans.* • *A third party could perhaps manipulate the contents of this study for their political purposes.*

6. **Have you documented why you are collecting the specific items of information to demonstrate they are necessary for your stated purposes** *e.g. if you are carrying out research into how students' music preferences affect their degree classification and also collecting participants' shoe sizes, can you show you have a legitimate need for this information, when they are not obviously linked?*	Yes	*Please provide details: In the Participant Information Pack, participants have been notified of why they are being interviewed and how their interview transcripts will be primary data sources for use in the final write-up of the thesis.*
7. **Have you written an appropriate privacy notice to provide to individuals at the point you collect their personal data?** *A privacy notice is a legal requirement and tells individuals how you will process their data if they give it to you, among other things. Clear and detailed guidance about privacy notices and what they must contain is available here. If you are carrying out research, you should refer participants to the University's standard privacy notice for research participants, which must be supplemented by your participant information sheet.*	Yes	*It is confirmed here that this research will be using the standard privacy notice.*

Consent

Consent to participate in a research study is not the same as relying on consent as a lawful basis on which to process personal data. Researchers are strongly discouraged from relying on consent as a lawful basis for processing personal data for research purposes.

If you are relying on consent as the lawful basis for processing personal data, the GDPR requires that a certain standard of consent is obtained. Consent as a lawful basis to process personal data is only valid if it is freely given, fully informed, unambiguous and **capable of being withdrawn at any time**. If consent is withdrawn, you must cease all processing of personal data which is being carried out on the basis of that consent. For research purposes, this means that if a participant withdraws consent to process their personal data, all processing must cease and all personal data already collected about that participant must be deleted or destroyed. This may have significant implications for your research.

The GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). A failure to respond to a notification that an activity will take place unless an individual opts out is not valid consent. The GDPR also requires granular consent options for distinct processing operations e.g. participants may consent to you processing their survey responses but they may choose not to consent to you taking photographs of them during focus groups.

Consent should be separate from other terms and conditions. You must keep clear records to demonstrate consent has been obtained. You need to tell people about their right to withdraw and offer them easy ways to withdraw consent at any time.

You may still obtain participants' consent to participate in various aspects of your research, even if you do not rely on consent as a lawful basis for processing the personal data you subsequently collect. Participants may withdraw their consent to participate in any future aspects of the research but you may continue to process any personal data already collected **if** you have relied on a lawful basis for processing other than consent.

Further detailed information about obtaining valid consent under the GDPR is available here.

8. **Have you checked and confirmed that consent is necessary and is the most appropriate basis for your processing?** *Note that this question relates to consent as a lawful basis for processing personal data and **not** consent to participate in your research.*	Not applicable	*Please provide details:*

9. **If you are processing special category data or criminal convictions data on the basis of consent, have you planned to obtain individuals' explicit consent?** *As the standard for consent is so high under the GDPR, there is not likely to be a significant difference between consent and explicit consent.*	Not applicable	*Please provide details:*
10. **If you are relying on individuals' consent as the lawful basis for using their personal data, have you developed a process for managing the withdrawal of consent at any point during or after the research?**	Not applicable	*Please provide details:*
11. If you are relying on consent as a lawful basis to process personal data, have you ensured that the individual understands their rights and is capable of giving consent? This should be assessed on a case-by-case basis. *If you are processing personal data about children or those with reduced capacity, consider whether or not you need to obtain consent from parents, guardians or legal representatives. You must consider how to provide clear consent statements to those whose first language is not English.*	Not applicable	*Please provide details:*

Security

The GDPR requires you to process personal data securely. This means that you must have appropriate security measures in place to protect the personal data you hold from being lost, damaged, destroyed or disclosed inappropriately. Security measures include technical security measures to keep electronic information secure; physical security measures to keep hard-copy information secure; and processes and procedures around the management of, and access to, the information.

Organisations can be fined up to €20 million for breaches of security involving personal data. The GDPR requires us to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. It is important that any personal data you collect or use during your activities remains secure until it is securely destroyed, which includes ensuring that only those who are authorised to access and use the data can do so.

For further guidance on information security, please see the Information Governance pages of the UCLan intranet and the LIS IT Security Policy. You may also find the information on the ICO website useful.

12. **If you are intending to publish information which could identify individuals, have you made those individuals aware that this will happen via your privacy notice and obtained their consent, if appropriate?**	Yes	*Each participant has been notified via their receipt of the Participant Information Pack that there are two categories of participants for this study split between anonymous participants and non-anonymous participants. The category of which they are part will be discussed prior to their acceptance to participate in the research. Participants will be anonymised if they are not a public figure (e.g. commissioner) in the field of religious freedom and either have in the past or are continuing to experience impacts caused by religious recognition misuse on their right to religious freedom. To protect the safety of these individuals, anonymity will be granted to them. Participants in Category One are known figures in the field of religious freedom or are leaders of a religious group who represent their community and will speak in such a capacity. Therefore, this category of participants will not be anonymised as per the justification found in the original ethics submission from April 2021. This topic of anonymity is addressed on page 10 in the PIP.*

13. **Will papers, files, audio visual recordings, CDs, USB (memory) sticks, microfiche or other media which contain personal data be kept in locked cabinets, cupboards, drawers etc. when the offices are vacated or if they are stored off UCLan premises?**	Yes	*On page 7 of the Participant Information Pack, it is explicitly stated to participants that their interview recordings and transcripts will be kept in a password-protected folder accessible only by the researcher for up to five years after the research has been conducted. This is to be consented to in section 4 in the study's Consent Form.*
14. **Do all individuals who will have access to or be using the personal data understand that it must not be provided to any unauthorised person (which includes disclosing information to family members or other representatives of data subjects, unless the data subject has given consent for us to do this)?**	Yes	
15. **Do all individuals who will have access to or be using the personal data understand their responsibilities under data protection legislation and have they received data protection training?** *A GDPR e-learning course is available to staff and students via Blackboard.*	Yes	

16. Do you have appropriate procedures in place to ensure the security of the personal data if it is removed from or collected and stored away from UCLan offices for any reason? *You must provide details of how you will ensure personal data remains secure if you remove it from UCLan premises or collect and store it away from UCLan premises. Please note that electronic data must only be removed if it is stored on encrypted devices or media e.g. an encrypted disc or USB stick, an encrypted laptop or Dictaphone etc. Alternatively it can be accessed remotely via a secure connection. If an unencrypted device containing personal data is lost or stolen, it is likely to lead to a substantial fine for a breach of data protection legislation. Non-electronic records must be rigorously safeguarded at all times and not left unattended or in view of unauthorised people. Laptops, USB sticks and other devices, papers or any other form of personal data must not be left in cars.*	Yes	*Participants are made aware on page 7 of the Participant Information Pack that their information will be stored on a folder that is password-protected and is accessible only to the researcher. This folder will only exist on the personal laptop computer of the researcher which is itself password protected in order to provide double security.* *The interviews take place via the programme Microsoft Teams under the UCLan account which is password protected. Additionally, the internet router for where the interviews will take place is also password protected which means that no third party can view my interviews while they are taking place over the internet.*
17. **Will the personal data be stored on the UCLan network, or in an Office 365 account provided by UCLan, in a secure location with restricted access, to prevent unauthorised parties who have no right or need accessing the data?**	Yes	*Please see page 7 of the Participant Information Pack for further details.*

18. **Are all individuals who will have access to or use the personal data aware that personal information should only be stored on the UCLan network or in cloud storage provided by UCLan and should only be stored on equipment owned or leased by UCLan, unless exceptional circumstances apply, after taking advice from LIS?** *Storage under such exceptional circumstances must include the use of appropriate security measures. No personal information should be stored on any removable media e.g. USB sticks, CDs or devices e.g. laptops, smartphones, Dictaphones unless they are encrypted. BitLocker is the recommended tool for encrypting external devices; guidance can be found here. UCLan makes available Office 365 cloud storage for staff and students, including OneDrive for Business. This is the only approved cloud storage facility.*	Yes	

19. Are all individuals who will have access to or use the personal data aware that any information accessed via remote working methods such as Outlook Web App, UCLan Global or similar must be treated securely in line with relevant legislation and all University guidelines? *UCLan business information, including personal data, should not be stored on personal, non-UCLan equipment or devices unless exceptional circumstances apply, after taking guidance from LIS, even where personal equipment and devices are used to access information remotely. See the BYOD Policy for further information.*	Yes	
20. **Are all individuals who will have access to or use the personal data aware that email is not a secure method of communication and can easily be sent to the wrong recipient and do they know how to encrypt documents so that they can be attached to an email and sent securely?** *N.B. Encryption passwords must be provided separately and never included in the same email as the encrypted attachment. Guidance is available here. Users should consider whether or not email is the most appropriate method. Consider using UCLan's OneDrive for Business instead.*	Yes	

21. **Are all individuals who will have access to or use the personal data aware that all non-electronic material which contains personal data and has been authorised for disposal must be disposed of via the University's confidential waste service (including handwritten notes, computer print-outs etc.)?**	Yes	
22. **Are all individuals who will have access to or use the personal data aware that any paper documents, electronic media or hardware which has been designated for disposal must be kept in a secure location until it has been appropriately destroyed and any information it contains is no longer accessible or recoverable?** *Electronic media and hardware must be disposed of in line with LIS guidelines and procedures.*	Yes	

23. **Data protection legislation prohibits the transfer of personal data to countries or territories outside the European Economic Area (EEA) unless certain conditions can be met. Can you confirm that if you intend to transfer personal data outside the EEA, you have taken advice from the Information Governance team to ensure you can do so in compliance with data protection legislation?** *Transfers includes via email, websites and by virtue of using 'cloud' providers which store your data on their servers based overseas, as well as physically holding the information overseas. For detailed guidance see Sending personal data outside the UK.*	Yes	

Third parties acting on behalf of UCLan
Under some circumstances, it will be necessary or desirable to work with organisations external to UCLan, such as charities, research organisations, private companies, other public sector organisations, contractors, service providers or any other types of third parties. If a third party is acting on our behalf e.g. providing a service for us or on our behalf and that activity involves the third party accessing, collecting or otherwise processing personal data, they are a *data processor* under the GDPR. Guidance on the use of data processors, including a checklist to ensure their use is appropriate, is available here.

24. Are you using a data processor?	No	*If no, then you do not need to complete the questions regarding data processors below.*

25. **If you are using a data processor or you need help deciding if the proposed arrangement does involve a data processor, have you read the guidance and, if necessary, taken advice from the Information Governance team to ensure all data protection requirements around the use of data processors have been satisfied?**	Yes/No	*Please provide details:*
26. **If you are using a data processor, have you taken advice on information security from the Information Governance team and the Information Security team in LIS?** *It is a legal requirement to ensure a data processor is capable of putting in place appropriate technical and organisational security measures to protect personal data. If your data processor is based outside the EEA, additional measures must be in place.*	Yes/No	*Please provide details:*
27. **If you are using a data processor, have you taken advice from the contracts team in Legal and Governance or from Procurement (as appropriate) to ensure you have appropriate contractual arrangements in place to cover the use of a data processor?** *It is a legal requirement to have GDPR-compliant contracts in place with data processors.*	Yes/No	*Please provide details:*

Once this form has been completed, it should be attached to your Ethics Application Form (if applicable) and submitted as directed. If your activity does not require further or any ethical approval, this form should be retained with your project documentation as a record of your

considerations and data protection compliance. If you require any further advice or guidance to help you complete this checklist, please contact the Information Governance team: DPFOIA@uclan.ac.uk. Members of staff can also find a variety of guidance documents and FAQs on the Information Governance intranet pages.