EDINBURGH Nnapier UNIVERSITY

DATA PROTECTION LEGISLATION (GDPR AND DPA 2018)

STAFF CHECKLIST FOR SYTEMATIC DATA SHARING WITH THIRD PARTIES

NO.	ISSUE	QUESTIONS TO CONSIDER	RESPONSES/ COMMENTS	√
1.	Justification for sharing	• What is the data sharing meant to achieve • Have the potential benefits and risks to individuals of sharing or not sharing been assessed • Is the data sharing proportionate to the issue being addressed • Could the objective be achieved without sharing personal data e.g. by anonymisation		
2.	Power to share	• What is the nature of the information you have been asked to share • What are the University's relevant functions or powers to engage in this proposed data sharing		
3.	Identify the actors	Who will be providing, obtaining, recording or holding the personal data that will be shared.		
4.	Define the purposes	• What is the purpose of the data sharing • Does it fall within the broad purpose for which the data was originally collected or is it a new purpose.		
5.	Determine the data protection roles	• Will the third party with which data is to be shared be a data processor, a joint data controller, or a data controller in common • Do they understand the data protection implications of their role.		
6.	Consider the categories of personal data	Is the scope of the personal data to be shared adequate, relevant and not excessive as regards the purpose.		
7.	Identify Special Category Data or data relating to criminal convictions	Is the personal data to be shared data relating to racial or ethnic origin, political opinions, religious beliefs,		

		membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.		
8.	Identify the processing conditions	Based on whether data is 'special category' or not, can the data sharing can be supported by one of the required processing conditions.		
9.	Choose processing conditions	If the purpose for the data sharing could be capable of justification under a number of the conditions, which condition is to be relied upon (refer to s.8.1 of the Data Protection Code of Practice		
10.	Consent of the Data subject	• Will this be required for the data sharing to be lawful • Has it been obtained and if not, how will it be obtained.		
11.	Inform data subjects	• Is there a Privacy Notice in place or is the sharing covered by the Staff or Student Privacy Notices • Based on the information they were given when the data was collected, could the data subjects reasonably expect their personal data to be used for the purpose for which it is proposed to share it. • Could they reasonably expect their personal data to be shared with the third party in question • Could the data sharing cause substantial and unwarranted damage or distress to the data subjects and how you will respond to any objections you may receive • Will they need to be informed of the data sharing by the third party.		
12.	Data security	• Are there adequate technical security measures in place to protect the data from loss or unauthorised disclosure not only when held in the University but also in transit to a third party • Consider the effect a breach of data security could have on the individuals or on the University		

		• How will the data be shared		
13.	Data subject access	• Have the data subjects been provided with sufficient information to exercise their data protection rights, including the right of access to data held on them. • Can they identify the Data Controller or Controllers who will be sharing their data, and against whom their rights can be exercised		
14.	Contractual agreements between actors	• Is the nature of the data sharing such that it would be sensible to have a formal agreement between the initial data controller and the third party. • Should such an Agreement be a Data Sharing Protocol, a Joint Data Controllers Agreement or a Data Processor Agreement		
15.	Institutional Framework	Do the initial data controller and the third party have in place suitable practice and procedures to meet their data protection obligations		
16.	Retention periods	Are there agreed common retention periods for the data to be shared		
17.	Secure Disposal	Are there processes in place to ensure the secure disposal /destruction of the data		

Once completed send to Governance Services for review dataprotection@napier.ac.uk

This table has been prepared from the JISC Model Code of Practice (2008)
Governance Services/ revised in March 2019