Data Protection Impact Assessment (DPIA) Policy

Version: 2
Date: 08.03.2019
Authors: Caroline Pegg, Aimee Chambers.
Responsible Officer: Executive Director Customers and Change

Contents

1. Policy Statement

1.1. West Sussex County Council (WSCC) processes a significant volume of personal and special category data including data relating to children and vulnerable adults.

1.2. In compliance with Article 25 of the GDPR WSCC adopts internal policies and implements measures which meet the principles of data protection from the initiation of new projects and service change proposals. This policy describes how we embed good practices into WSCC.

1.3. Adhering to this policy, using the enclosed Screening Questionnaire (SQ) and DPIA template, we will be able to identify when a DPIA is required and/or appropriate and record the process through to completion of a DPIA and its ratification.

1.4. For the policy to be its most effective, it must be followed at the very early planning stages of new projects and run alongside the project plan.

2. Scope

2.1. This Policy shall apply to any department/service which is introducing a new or revised service or changes to a system, process or information asset which includes processing personal data.

2.2. Project Managers, Contracts and Procurement, Research and consultation, and IT services should have particular regard to this policy.

2.4 WSCC shall ensure that our partner organisations and contractors shall have a legally compliant DPIA policy or adopt this policy. This Policy shall apply and will be transmitted to our partners and contractors and it shall be the responsibility of the Data Protection Officer to embed this policy and approach to data protection in all of our formal business with partners and suppliers.

3. Definitions

Personal Data: any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Data: Special category data (previously referred to as Sensitive Personal Data) means personal data consisting of information as to any of the following:-

- racial or ethnic origin
- political opinion
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- genetics;
- biometrics (where used for ID purposes);
- physical or mental health or condition
- sexual life or sexual orientation.
- personal data relating to criminal allegations, proceedings or convictions.

Processing: any operation or set of operations which is performed on 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 communication, restriction, erasure or destruction.

High Risk Data: Highly sensitive personal data including special category & criminal data.

Criminal Data – applies to the personal data relating to criminal convictions and offences, criminal allegations and proceedings. GDPR extends the definition to personal data linked to related security measures.

Screening Questionnaire is the process documented at Appendix 2 to this Policy.

4. Duties and Responsibilities

Responsibilities of the officers

Leadership

- The Chief Executive shall be accountable for the implementation and effectiveness of this policy.
- Executive Directors and Directors are responsible for implementing this policy and associated procedures within their services and operations of those services.
- The Information Security Management Group (ISMG) should oversee the effective operation of this policy.

Data Protection Officer & the Data Protection Team

- To ensure implementation of this Policy
- To review this policy regularly
- To monitor compliance with this policy
- To report to the Chief Executive on the effectiveness of this policy.
- Ensuring that Data Protection is included at the earliest possible stages of and embedded in projects.
- Providing support to the those undertaking DPIA's

Employees involved in processing of personal data

- It is the responsibility of all staff to ensure that their working practices comply and consider this policy.
- To complete a DPIA when legally required or it is appropriate to do so

5. Main Policy Content

Introduction to DPIAs

Officers working on any new project or service change initiative which will include the processing of personal data shall use the DPIA flow (appendix 1) and, if required, ensure that a DPIA is completed.

A DPIA is a systematic process which will help identify and minimise data protection risks. DPIAs shall consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

A DPIA should help to minimise risks and assess whether or not any identified risks are to be tolerated in line with **WSCC – *Risk Management Strategy***

DPIAs are a legal requirement for processing that is likely to be high risk. Failing to carry out a DPIA in these cases may leave WSCC open to enforcement action, including a significant fine. Working through the policy's supporting document will identify when a DPIA is legally required and/or appropriate.

5.1 DPIA Flow

5.1.1 Appendix 1 (DPIA Flow) contains the flowchart for the whole process. There are essentially three elements.

(1) Identification that a project involves personal data & nominating a responsible person.

(2) Completing a Screening Questionnaire (Appendix 2 – Annex A) to identify if a DPIA is required

(3) Completion and Sign Off of the DPIA. (Appendix2 – Annex B)

5.2 Screening Questionnaire (SQ)

5.2.1 Following the workflow, the responsible person shall complete the Screening Questionnaire.

5.3. Privacy Impact Assessment (DPIA)

5.3.1. If the Screening Questionnaire identifies that a DPIA is required and/or appropriate the responsible person shall complete the DPIA.

6. Monitoring Compliance

6.1 Adherence to this Policy will be monitored by the Council's ISMG.

6.2 The Data Protection Team shall assist the ISMG in reporting on compliance.

6.3 Each Director/head of service shall monitor compliance with this policy.

6.4 It is the responsibility of the Data Protection Team to audit completed DPIA's six months following their completion to ensure risk mitigation measures were implemented in to the project.

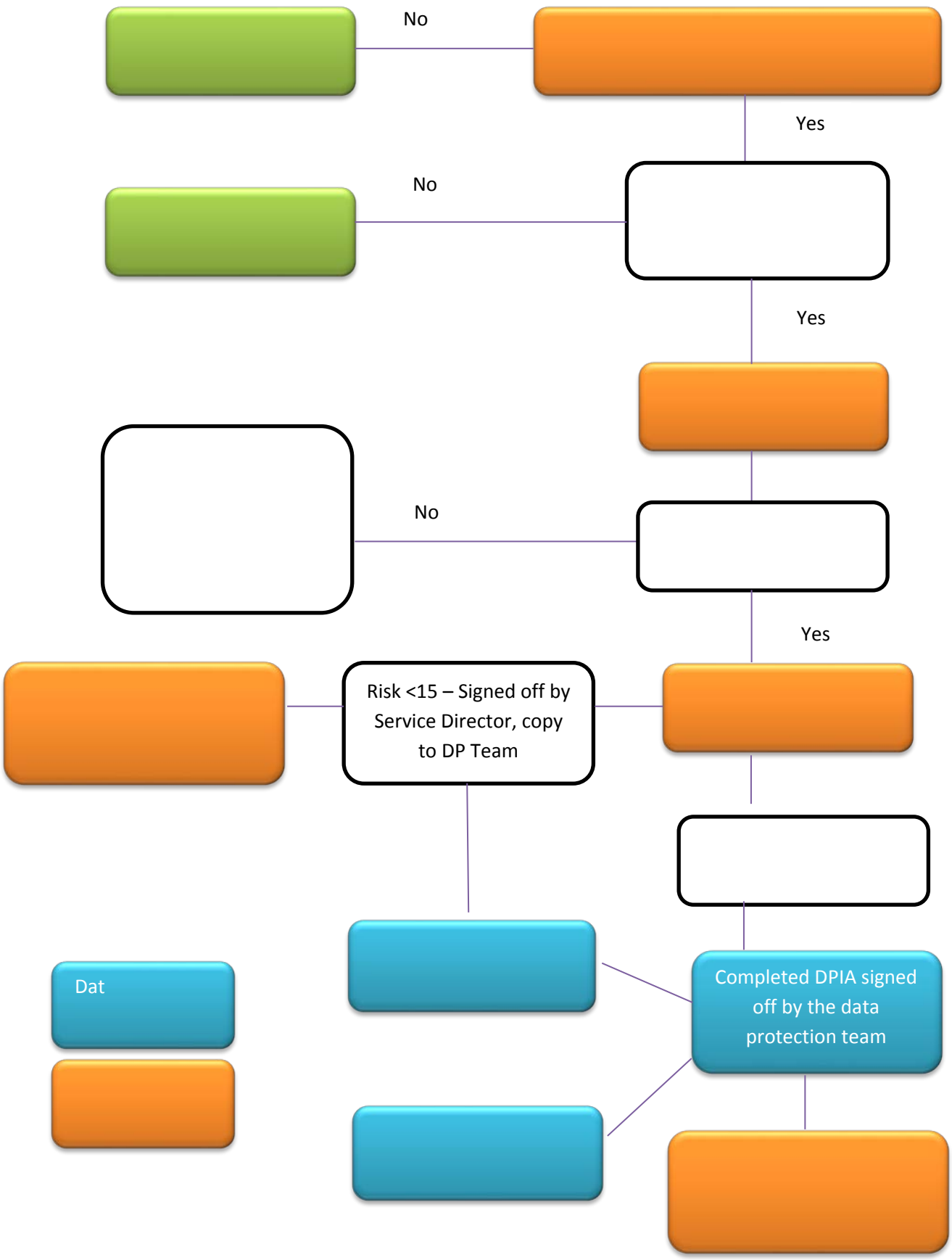
7. Associated Documents

Data Protection Policy

West Sussex County Council Risk Management Strategy

Data Sharing Policy

Appendix 1 – Data Protection Impact Assessment Flow



Appendix 2 – DPIA Screening Questions

DPIA Screening Questions	DPIA Required?	Example
Are you planning to use **Innovative technology** or **applying new technological or organisational solutions?**	1. Processing involving the use of new technologies, or the novel application of existing technologies (including AI). **– DPIA required** 2. **A DPIA is required** for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions **when combined with any other criteria below**)	Fingerprint recognition technology to access a building, face recognition, AI, connected/autonomous vehicles, smart technologies, intelligent transport system
Does the project involve evaluating or scoring **individuals (including profiling and predicting) –** See DPIA guidance for info on profiling	**DPIA required**	Building behavioural or marketing profiles of individuals based on their web activities. Credit reference databases, genetic tests to predict health risk. Performance at work/health/location
Does the project involve **automated decision making** that might have a significant legal effect on an individual **-** See DPIA Guidance for info on automated decision making.	**DPIA required**	Asking an individual to submit personal data that is then analysed by a computer system, with the result that the individual's request to use a service is either accepted or refused
Does the project **prevent individuals from exercising a right or using a service or contract? (Denial of Service)**	Decisions about an individual's access to a product, service, opportunity or benefit which are based on any extent to automated decision making (including profiling) or involves special category data - **DPIA required**	Screening applicants before allowing them to use a service/bank screening customers against a credit reference in order to decide to offer them a loan, mortgage/insurance applications
Does the project involve **systematic monitoring/tracking?**	Observe, monitor or control data subjects, including data collected through networks or a systematic monitoring of a publicly accessible area. This type of monitoring requires a DPIA because the personal data may be collected in circumstances where data subjects may not be aware. Additionally it may be impossible to avoid being subject to such processing in public - **DPIA required**	Processing used to observe, monitor or control individuals - Installing a CCTV system, tracking location (online and offline), consider mobile apps which monitor health data
Does the project involve the processing of **sensitive/special category or Criminal data**? **–** See DPIA guidance for info on types of data		Processing of health data of residents in a joint project with another authority, new projects,
	There is no specific definition of 'large scale' but the following should be considered: • The number of individuals affected • The volume of personal data • The range of personal data • The duration or permanence of the processing activity • The geographical extent of the processing activity. **DPIA required when combined with another criteria.**	Creating a new service
	This relates to combining personal data originating from two or more personal data processing operations performed for different purposes or by different	Fraud Prevention/direct marketing/monitoring personal use/uptake of statutory services or

	data controllers in a way that would exceed the reasonable expectations of the individual – **DPIA required**	benefits/federated identity assurance services
Does the project involve the **personal data of vulnerable people?**	This relates to the processing of personal data where there is an imbalance of power between the individual and the Council, or the processing involves a vulnerable section of society - **DPIA required**	Processing children's personal data, power imbalance between the data subject and the Council, employees, requiring special protection/connected toys/social networks
		Whistleblowing/complaint procedures/social care records/safeguarding enquiries/criminal data
		Facial Recognition/workplace access/identity verification/access control/fingerprint & facial recognition) Genetic data – medical diagnosis/DNA testing/Medical Research

Completed by:…….

Service:

DPIA required: Yes/No

If a DPIA is **not required** please detail your project plan and send to dataprotection@westsussex.gov.uk for logging and final assessment.

If a DPIA **is required** complete the below template.

Project Details

Project Name	
Project Title	
Implementation Date	
Name of Controller	
Name of Processor (if applicable)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures: *what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? **How will you help to support their rights?***What measures do you take to ensure processors comply? How do you safeguard international transfers?

*We have provided some tables below to assist you with the questions marked */** and ***. You will still need to answer the other questions being asked.*

Lawful basis for Processing **(General Processing)**

Personal Data (Select one) *Example: name/date of birth/address/bank details/IP address*	☑	**Special Category Data** (select one) *Notes - Race/ethnic origin/politics/religion/trade union membership/genetics/biometrics/health/sex life/sexual orientation* *You will need to have selected an Article 6 basis before selecting your Article 9 basis*	☑	**Criminal Data** (Select one more) *Notes – Criminal allegations, proceedings or convictions* *You will need to have selected an Article 6 basis before selecting your DPA 2018*	☑
Consent		Explicit Consent		DPA 2018 Sch 1 Part 1	
Contract		Employment and social security and social protection law		DPA 2018 Sch 1 Part 2	
Legal Obligation		Vital Interests		DPA 2018 Sch 1 Part 3	
Vital Interests		Not for profit		Appropriate Policy Document – DPA 18 Sch 1 Part 4	☑
Public Task		Manifestly made public by the data subject			
Legitimate Interests		Establishment, exercise or defence of legal claims			
		Substantial public interest (Sch1 DPA 2018)			
		Health or social care treatment			
		Public interest in area of public health			
		Archiving in the public interest			

Lawful basis for processing **(Law Enforcement Processing (Part 3 Data Protection Act 2018) e.g. trading standards and truancy prosecutions)**

Personal Data (Select one) *Example: name/date of birth/address/bank details/IP address*	☑	**Special Category Data (DPA Part para 35)** *Notes -* *Race/ethnic origin/politics/religion/trade union membership/genetics/biometrics/health/sex life/sexual orientation* *You will need to have selected an Article 6 basis before selecting your Article 9 lawful basis.*	☑	**Criminal Data** *Notes –* *Criminal allegations, proceedings or convictions*	☑
Consent		Consent		Section 42 DPA 2018	☑
Processing is necessary for that purposes by a competent authority		Strictly necessary for law enforcement purposes + schedule 8		Must have statutory function (Part 3 para 30(1)(b)	

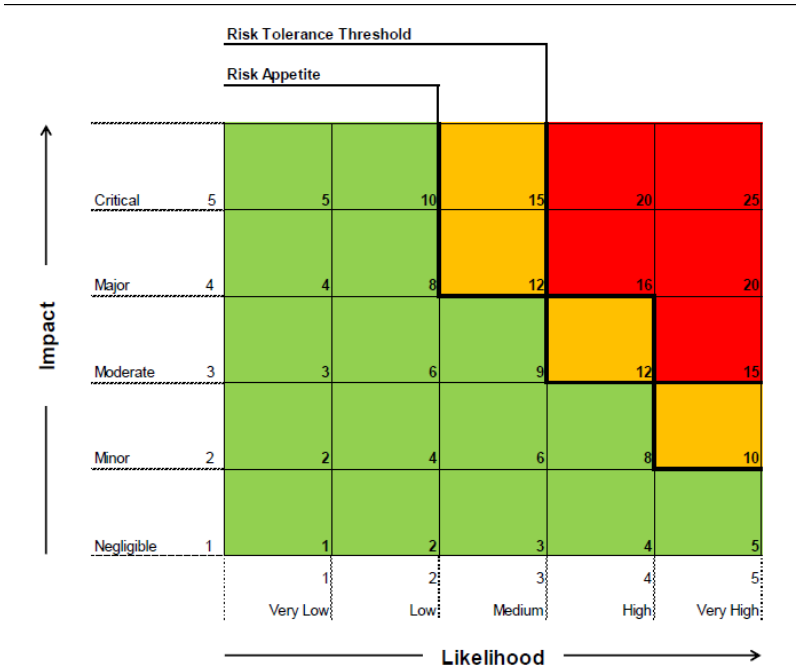
**Rights of individuals

Right	Data Subject able to exercise right	Measure/If not, why?
Right to Be informed	Yes/No	
Right of Access	Yes/No	
Right to Erasure	Yes/No	
Right to restrict processing	Yes/No	
Right to data portability	Yes/No	
Right to Object	Yes/No	
Rights in relation to automated decision making and profiling	Yes/No	

***What measures will you take to ensure Processors comply?

Article 28 clauses within Contract	Yes/No
Completed Data Security Questionnaire (IT Services)	Yes/No
Will the Processor be able to comply with individuals rights	Yes/No

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks	**Likelihood of harm**	**Impact of harm**	**Overall risk**
Use the WSCC Risk Matrix and Guidance - http://teamspace.westsussex.gov.uk/teams/BI/Performance/rm/Shared%20Documents/Risk%20Management%20Documentation/Risk%20Management%20Guide/WSCC%20Risk%20Management%20Guide_V2.1.pdf  Employee negligence & error/Cyberattack/unauthorised access/Physical theft & exposure/Insider threat/Phishing	Very low/low/medium/high/very high	Negligible/minor/moderate/major/critical	

Examples			
1. An employee may gain unauthorized access to the system, accessing personal data inappropriately. Either via password sharing or IT system error.	Low	Major	8
2. A user may download the data and use it for an unauthorized purpose.	Medium	Major	12
3. An outside agency tries to access the data (hacking)	Medium	Major	12
4. Data not being backed up, data which is lost is not capable of being retrieved	Medium	Major	12
5. An employee changes sensitive data for their own purposes	Low	Moderate	6
6. Personal Sensitive Data is being shared with multiple parties in a joint project and there is the possibility of it going to the wrong place or ensuring the compliance of data protection of the other parties	Medium	Major	12
7. CCTV will be installed within library (risks breach of the right to privacy)	Medium	Moderate	9
8. Inadequate functionality (risks: not able to locate/delete records)			
9. ….			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Examples		Eliminated reduced accepted	Low medium high	Yes/no
1. An employee may gain unauthorized access to the system, accessing personal data inappropriately. Either via password sharing or IT system error.	Data Protection Policies/Acceptable Use Policies/HR Staff have full training in protecting their user accounts and accessing personal data in private areas. Password policy is enforced. WSCC have protective monitoring in place to detect abnormal user account access.	Reduced	Low	Yes
2. A user may download the data and use it for an unauthorized purpose.	Removable devices disabled/control only for managers to download data	Reduced	Low	Yes
3. An outside agency tries to access the data (hacking)	Firewalls/Anti-virus/encryption at rest/Secure settings on the software/passwords/dual factor authentication/Whitelisting/sandboxing/Patching	Reduced	Low	Yes

4. Data not being backed up, data which is lost is not capable of being retrieved	Back ups included as a necessary requirement in the specification of the project	Eliminated	Low	Yes
5. Employee changes sensitive data for their own purposes	WSCC have protective monitoring in place to detect abnormal user account access. The technology will ensure that there is a trace and auditing function	Reduced	Low	Yes
6. Personal Sensitive Data is being shared with multiple parties in a joint project and there is the possibility of it going to the wrong place or ensuring the compliance of data protection of the other parties	1. Completion of a data sharing arrangement, including expected data security standards 2. Ensure the data is encrypted in transit, password protected 3. Limit access to data on a need to know basis/privileged access	Reduced	Low	Yes
7. CCTV is installed in library	1. Ensure CCTV complies with ICO CCTV Code of Practice 2. CCTV signage is lawfully placed and privacy notices will be placed at all entry	Reduced	Low	Yes

	and exit locations to the building 3. Material is retained for 30 days (unless evidence) 4. Procedures and processes in place with regards to access, monitoring and use. Use of system will be fully auditable and traceable 5. Data location is alarmed with electronic access control and limited to 5 members of staff 6. Etc….			

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	If risks are within the WSCC risk appetite (green), measures can be approved by the Service Director & returned to dataprotection@westsussex.gov.uk	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	If risks are outside the WSCC risk appetite (i.e.amber and red), measures can be approved by the Service Director & returned to dataprotection@westsussex.gov.uk	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	If risk is above Risk appetite, measures need to be approved by DPO.	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA