Enabling Guidance

Document title: Commercial Data Handling

Document Reference: 15/332

Owner: Head of Department, Finance and Business Services

Review date: November 2022

This enabling guidance is suitable for public disclosure under the Freedom of Information Act 2000

This document sets out principles to help guide decision making and in some parts may be quite prescriptive. However, it is vital that officers and staff have the freedom to innovate, exercise discretion and take risk based decisions centred on the needs of the victim and the merits of each case.

There may be occasions when a member of staff is considered to have acted outside of the content of this document but if they have done so with honesty, integrity and professionalism, to make the best decision for the community we serve, they will be trusted and supported. On the occasions when this is the case, the rationale for it must be properly recorded.

This document should be read in conjunction with the Force Policy Statement.

Introduction

Aims and objectives

The force has a variety of information assets which are essential to the effective and efficient operation of the organisation and the delivery of its strategic aims and objectives. The force has a duty and legal responsibility to protect hose information assets (see definitions), which include personal data, whilst ensuring that information is used effectively for the public good. This applies equally where information may be managed or processed by third parties.

Information Asset Owners (IAOs) have a responsibility for understanding what information is held, what is added, what is removed, how information is moved and who has access and why. They will therefore be best placed to understand the impact of any breaches of force policies and have a duty to ensure compliance with these policies.

The Procurement Unit, Finance and Business Services will work with suppliers to increase their awareness of appropriate force policies. They will also ensure contracts reflect operational requirements relating to information assets as advised by IAOs.

The Cabinet Office has stipulated that it is mandatory requirement that a number of standard contract clauses, relating to security and information assurance, are adopted in all new contracts. These mandatory provisions have been incorporated into a series of schedules, the applicable one of which for each supplier will form part of the contract with that supplier. This approach acknowledges that different suppliers will have different levels of access to data and systems of the force whilst performing their obligations and that therefore, different measures will be required. As a consequence, there are four different categories with different levels of requirement as follows: -

- Category 1 – suppliers who process and store personal data and police data outside force systems;
- Category 2 – suppliers who process and store police data excluding personal data outside force systems;
- Category 3 – suppliers who have access to police data within force systems; and
- Category 4 – suppliers who simply supply the force with goods or have access to unclassified police data.

Guidance

Categories 1 – 4 schedules explained

All the versions of the schedule include basic confidentiality protections, Freedom of Information Act (FOIA) cooperation provisions and audit requirements. Such measures suffice for Category 4 suppliers. In addition categories 1, 2 & 3 also include: -

- Various general requirements designed to preserve the security and integrity of the force's data;
- Basic obligations to ensure compliance with the Data Protection Act (DPA) and that any processing carried out by suppliers is in compliance with the force's instructions;
- An obligation to comply with the force's security policy (as updated from time to time); and
- Staff vetting requirements.

Categories 1 and 2 also include: -

- More specific requirements relating to preservation of the security and integrity of the force's data (for instance in relation to encryption and taking back up copies);
- More detailed DPA obligations, including a requirement to implement appropriate technical and organisational measures to protect personal data;

- A requirement to implement more wide-ranging security principles, including ensuring compliance with ISO 27001 best practice information security management; and
- A requirement to undertake regular assessments.

Category 1 also includes: -

- A requirement to develop, implement and maintain a specific security plan for the services the supplier provides to the force, that has to be approved by the force. The supplier must obtain and maintain independent certification of the plan to ISO 27001; and
- An obligation to maintain a business continuity and disaster recovery plan in relation to the performance of its services to the force and the availability of related ICT systems and data. This must be subject to regular testing which the force can observe.

Applying the schedules

There may be some contracts for which it is clear that the use, dissemination or other handling of personal and/or confidential information is a clearly identifiable part of delivering the contractual requirement e.g. personal details/records of participants on force programmes shared with a supplier to conduct evaluation research/interviews. A decision must be taken by the IAO as to what category of data handling schedule should be included to address any information risks.

Category of data handling schedule (examples)

Category of data handling schedule		**Description**	**Example of contracts**
1	Suppliers who process and store personal data and police data **outside** of force systems.	Providers who store and process personal data on their own ICT systems.	Out sourced contract for payroll.
2	Suppliers who process and store police data excluding personal data **outside** of force systems.	Suppliers who are provided with police data to store off site and on their own ICT systems.	Vehicle Recovery contract.
3	Suppliers who have access to police data **within** force systems.	Suppliers storing and accessing police data on force sites and via remote access.	Server maintenance contract.
4	Suppliers who supply the force with goods or services.	Suppliers who engage with the force, do not have access to police data and do not generate any police data as a result of their engagement. Or suppliers who have access to unclassified police data.	Stationery supplier, electricians, painters and decorators, speakers at conferences/events.

Things to consider

At the pre-tender (strategy) stage: -

- Use of police data is best considered at an early stage of any project i.e. at the point when a statement of requirement (specification) for work is being formulated for any procurement activity. This ensures that police data issues are considered and included in the overall procurement strategy for the project.

- What, if any, police data needs to be shared with a supplier in order for them to meet the requirement and successfully deliver the contract. Refer to the process above.
- Do not share police data if it is not material to delivery of the contract.
- Does police data need to be shared in their entirety or can elements be removed (e.g. names and addresses) thereby reducing the protective marking classification and therefore reducing the data handling requirements imposed on the supplier as part of the contract can be reduced.
- Will any police data be created during the supplier delivering the contract and if so what data classification will this need to have?
- How will police data, both existing and those created as part of the contract, be stored by and transmitted to suppliers. This must be appropriate to the classification of data.

At tender stage: -

- At the point the Procurement Unit are contacted and provided with a draft statement of requirement and budget approval, the IAO will need to have approved appropriate category of data handling schedule.
- Commercial will accept IAO approval of the data handling category in the form of an IAO signed scoping document or email from the appropriate IAO to the contact in Commercial leading the procurement.
- When bids are evaluated the category of data handling schedule must e reassessed to confirm whether initially identified category of data handling schedule still applies. The reason for this may be a supplier proposing use of police data not planned as part of the statement of requirement and procurement strategy.
- For contracts identified as being category 1, commercial will work with appropriate project members to seek assurance from potential suppliers that they either have or are working towards the required compliance with the category 1 data handling schedule.

At contract award/management stage: -

- Authorisation to commence work should only be given to the chose supplier once the contract is agreed and signed by all parties.
- Once the contract is signed and contract deliver commences it is the IAO's obligation to ensure police data is managed appropriate by suppliers throughout the life, termination and exit of any contract. Including destruction and/or return to the force of police data at the end of any contract.

Definitions

"Police Data" means any data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media and which: -

is provided to the Contractor by or on behalf of the force in connection with the Contract,

or

the Contractor is required to generate, process, store or transmit pursuant to the Contract,

or

is any Personal Data for which the force is the Data Controller.

"Personal Data" means data which relates to a living individual who can be: -

a) from those data OR

b) from those data and other information which is in the possession of, or likely to come into the possession of the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

"Processing" means information or Data obtained, recorded, altered, retrieved, stored disclosed or destroyed.

"Information Asset" means a definable piece of information, stored in any manner which is valuable to an organisation. There are several elements of value to be considered including the cost of replacing the information and the costs associated with loss of the information's confidentiality, availability and integrity. In its broadest sense information can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on film or (even) spoken in conversation.

Part 1 Human Rights

1. What is the policy or procedure title, what is its purpose or objective and who will be affected by it?
2. Will the policy or procedure restrict anyone's Convention rights?
If the answer to Q2 was Yes proceed to Q3. If the answer to Q2 was No proceed to Part 2, Equality Impact Assessment. However, be alert to any possibility that your policy or procedure may restrict someone's Convention rights, things may change and you may need to reassess.
3. What Convention rights are restricted? Are they absolute rights or limited rights?
4. What is the legal basis for the restriction?
5. What is the legitimate aim for the restriction?
6. Are the actions that restrict the right proportionate? Are you sure you are not using a sledgehammer to crack a nut?
7. Are the actions that restrict the right fair, non-discriminatory and least intrusive?
8. Does the policy or procedure specify that a record of any decisions that affect someone's rights are documented?
9. Has legal advice been sought on the policy or procedure?

DERBYSHIRE CONSTABULARY

Equality Impact Assessment

This form should be completed electronically and on completion forwarded to the Equality Unit mailbox.

This Equality Impact Assessment form must be used to inform your decision making when reviewing or developing new policies/guidance/procedure/ working practices. It should remain a live document and be reviewed at key milestones during development or at least yearly.

The General Duty

The general duty is set out in section 149 of the Equality Act 2010. In summary, those subject to the Equality Duty must have **DUE REGARD** to the need to:

- eliminate unlawful discrimination, harassment and victimisation, between those who share a protected characteristic and those who do not;
- advance equality of opportunity between those who share a protected characteristic and those who do not;
- foster good relations between those who share a protected characteristic and those who do not.

Authors have a statutory requirement to have **DUE REGARD** to the relevant protected characteristics shown below, whilst taking a common sense approach

- age
- disability
- gender reassignment
- marriage & civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex (gender)
- sexual orientation
-

Name of the policy/guidance, project or working practice (PGPWP):		Policy/Ref No:	

1. Briefly describe the intention of the PGPWP?

2. Does this PGPWP have a direct impact on people who :-		
a. Work for Derbyshire Constabulary (including specials and volunteers)	Yes ☐	No ☐
b. Reside or visit Derbyshire	Yes ☐	No ☐

3. How does what you are doing affect the following protected groups?

Include what relevant quantitative and qualitative data you have. This may include national/local research, surveys, reports, complaints and meetings. Please list any evidence in the boxes below.

Protected Characteristic	Impact or Benefits (include positives, as well as where risks are identified, if any)	Where risk is identified please detail what you can do to reduce this risk
Age		
Disability (physical, sensory, learning)		
Transgender (person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex)		
Race (Black, Asian, Chinese & Other, Mixed Race, White, Gypsy/Travellers, Asylum Seekers)		
Religion/Belief (Religion means any religion and a reference to religion includes a reference to a lack of religion. Belief means any religious or philosophical belief and a reference to belief includes a reference to a lack of belief)		

Sex (Gender) (men, women)		
Sexual Orientation (lesbian, gay men, bisexuals, heterosexual)heterosexual)		
Pregnancy and Maternity		
Marriage and Civil Partnership		

4. Who have you consulted with and what was their feedback? **Was their feedback adopted?** (If not why not?)

5. Is there any further consultation or engagement required?
No ☐ **Go to No.7** Yes ☐ **If Yes please contact the Equality Unit – Equality & Compliance Manager (75 04865) for advice on who to consult with.**

6. ACTION PLAN

This EIA will be reviewed on a yearly basis to monitor the impact on protected characteristics.

Following consultation and feedback what action will you take?

Action	**Timescale**	**Action Owner**

7. Quality Assurance - This assessment requires the signature of the EIA author. It should then be forwarded to the Equality Unit.

I am satisfied this assessment demonstrates compliance with the General Duties under the Equality Act 2010 , and that due regard has been given to the need to;-

- **Eliminate unlawful discrimination**
- **Advance equality of opportunity**
- **Foster good relations**

EIA Completed by:	**Date:**	**Department:**
PGPWP completed by:	**Date:**	
Head of Equality :	**Date:**	

This EIA will be retained until the next review date.

(Update when complete)
Choose an item. – Choose an item. – Choose an item.

Data Protection Impact Assessment (DPIA) – Stage 1

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material before completing the form.

Data Protection Impact Assessment (DPIA)	
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.	
Section 1 - Governance	
Project Proposal Name:	
Information Asset Owner:	
DPIA Coordinator: (Someone from the business area, a middle manager with a hands-on role with the project, heavily involved in its delivery.)	
Date on which processing will commence:	DD/MM/YYYY
Date submitted to the DPS: (Data Protection Section)	DD/MM/YYYY
Note: The DPS will give an **initial response** within 10 working days of receiving the completed form.	

DPS Assessment		
DPS Use Only		
A. DPIA is not mandatory.	☐	
B. A DPIA Stage 2 is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA Stage 2 will be required.	☐	
C. A full DPIA is mandatory.	☐	

Section 2 – Nature, Scope, Context and Purposes

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose(s) of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

2.3 Will special category data be used in the proposal? (Select all that apply)

☐ Race	☐ Trade union membership
☐ Ethnic origin	☐ Genetic Data
☐ Political opinions	☐ Biometric Data
☐ Sex life	☐ Sexual orientation
☐ Religion	☐ Health
☐ Philosophical beliefs	☐ None

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in Derbyshire Constabulary's possession, from a partner agency.

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

2.6 How many individuals will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects

☐ 100 to 1000 data subjects

☐ 1000 to 5000 data subjects

☐ More than 5000 data subjects

2.7 What categories of data subject are involved? (Please select all applicable categories below)

☐ Persons suspected of having committed or being about to commit a criminal offence

☐ Persons convicted of a criminal offence

☐ Persons who are or may be victims of a criminal offence

☐ Witnesses or other persons with information about offences

☐ Children or vulnerable individuals

☐ Derbyshire Constabulary staff (current and former)

☐ Other

If other then please provide further details below:

Click here to enter text.

2.8 Will it involve the collection of new information about individuals? Will Derbyshire Constabulary collect data that it has not previously collected or had access to?

☐ Yes
☐ No

2.9 Data Sharing **Does the processing involve:**		**Select one option**
2.9.1	Data being shared with third parties external to Derbyshire Constabulary or recipients that have not previously had routine access to the	☐ Yes ☐ No

	information?	
2.9.2	Transferring data outside the UK but within the EU?	☐ Yes ☐ No
2.9.3	Transferring data outside the EU?	☐ Yes ☐ No
2.9.4	Storing data using a cloud service provider?	☐ Yes ☐ No
2.9.5	Is there an MoU, contract, or other sharing agreement in place with all parties with whom data will be shared?	☐ Yes – agreements in place ☐ Not yet – agreements required ☐ No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?
For example, can the aim be achieved by using less data or different types of data? Are all categories of data necessary to achieve the aim?

2.11 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

Section 3 – Lawful Basis

3.1 Lawful Basis
To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Choose an item.

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes):

Choose an item.

3.2 Further Special Category Lawful Basis
If processing special category data (section 2.3) you must have identified a further lawful condition

Operational Data:
The processing is strictly necessary (please tick to confirm) ☐

AND

One of the following conditions applies (select from the list):

Choose an item.

Administrative Data
It is necessary for one of the following conditions (select from the list):
Choose an item.
OR

It is in the substantial public interest (tick to confirm) ☐

AND for the following purpose:

Choose an item.

Section 4 – Review, Retention and Disposal

4.1 Does the proposal have a review, retention and disposal process that complies with Derbyshire Constabulary Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within Derbyshire Constabulary's Review, Retention and Disposal Policy.

☐ Yes
☐ No

Section 5 – ICO: Additional Factors

The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.

	Does the processing involve:	**Please check either Yes or No**	**If 'Yes' then please provide further details**
5.1	**Systematic, extensive and large scale profiling and automated decision-making about people?** *"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"*	☐ Yes ☐ No	Click here to enter text.

	Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.		
5.2	**Large scale use of special category data or criminal offence data?** *"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"*	☐ Yes ☐ No	Click here to enter text.
5.3	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☐ Yes ☐ No	Click here to enter text.
5.4	**New technologies or techniques?** *"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"*	☐ Yes ☐ No	Click here to enter text.
5.5	**Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?** *"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"*	☐ Yes ☐ No	Click here to enter text.
5.6	**Biometrics/genetic data?** *"Any processing of biometric data"* ***and/or*** *"any processing of genetic*	☐ Yes ☐ No	Click here to enter text.

	data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject" Biometric data can include Facial Recognition technology, fingerprints and is defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.		
5.7	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☐ Yes ☐ No	Click here to enter text.
5.8	**Invisible processing?** *"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"* For example, when gathering data, without the knowledge of the data subject, in the course of a Derbyshire Constabulary investigation.	☐ Yes ☐ No	Click here to enter text.
5.9	**Tracking?** *"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"*	☐ Yes ☐ No	Click here to enter text.
5.10	**Targeting of children or other vulnerable individuals?** *"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children* For example, the use of personal data relating to children for the purposes of marketing their online	☐ Yes ☐ No	Click here to enter text.

	safety products.		
5.11	**Risk of physical harm?** *"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".* For example, if data relating to Child Sexual Abuse or Exploitation, Covert Human Intelligence Sources or protected persons data was compromised then it could jeopardise the safety of individuals.	☐ Yes ☐ No	Click here to enter text.
5.12	**Evaluation or scoring?** *"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of Derbyshire Constabulary's recruitment process.*	☐ Yes ☐ No	Click here to enter text.
5.13	**Data processed on a large scale.** *Considerations include:* • *The number of data subjects concerned* • *Volume of data and/or range of data items* • *Duration, or permanence, of the data processing* • *Geographical extent of data processing*	☐ Yes ☐ No	Click here to enter text.
5.14	**Preventing data subjects from exercising a GDPR right?** *The rights are:* • *The right to be informed* • *The right to access data* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to object* • *The right to portability* • *Rights relating to automated processing*	☐ Yes ☐ No	Right to be informed: What if any additional information does Derbyshire Constabulary need to provide to comply with Articles 12-14 and Section 44, which is not already covered in its Privacy Notices?

Please forward the completed form to Data Protection Team at DPROT@Derbyshire.PNN.Police.UK who will be able to assist further.

Part 3 - Consultation

1. What departments, individuals and organisations have been consulted in the development of this policy or procedure? At the very least you should consult with the below:- It may also be beneficial in some cases to consult with the Force Staff Network co-ordinator and Legal Services.

Name	Department / Organisation	Date
Police Federation		
Unison		
Data Protection		