Data Protection Manual



Prepared by Vikki Smith

Version: 1.4

Issue Date: Approved 20.04.2018

DAVENTRY DISTRICT COUNCIL

DAVENTRY DISTRICT COUNCIL

DATA PROTECTION MANUAL

Appendix II – Information Sharing Flowchart

Appendix III – Seven Golden Rules of Sharing Information

Appendix IV – Data Protection Checklist

Appendix V – Do I need to complete Data Protection Impact Assessment?

Appendix VI – Data Privacy Impact Assessment Template

Appendix VII - Security Tips

1. Introduction

1.1 Purpose

The purpose of this document is to assist employees with their understanding of the requirements of the General Data Protection Regulation 2016 (the "Regulation"), and other relevant data protection legislation.

1.2 Background

The General Data Protection Regulation 2016 (the "Regulation") regulates the holding and processing of personal data - that is information relating to identified or identifiable natural person, which is held either on the computer or in some cases in manual form. The Regulation also gives rights to individuals ("data subjects") whose personal information is held by organisations ("data controllers").

The Council needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective employees, suppliers, service users, residents and others with whom the Council communicates.

The Council, its processors, and in some circumstances its individual employees could face prosecution for failure to handle personal data in accordance with the Regulation.

1.3 Scope

This Manual is intended to be a practical document outlining the procedures to be followed when processing personal data. It is not to be treated as a detailed explanation of the law. You will find links to important policies, forms, to other websites and to supporting guidance.

Should you require a more detailed explanation of the law, please contact the Council's Data Protection Officer.

1.4 Data Protection Officer

The role of the Data Protection Officer is designated to the Governance & HR Manager. The Data Protection Officer has the following responsibilities:

- To act as Data Protection Officer, with overall responsibility for the processing and management of personal data
- Develop, and maintain the Council's Data Protection Policy and Manual
- Identify the Council's training needs and ensure appropriate delivery
- Identify, monitor and advise on information sharing and data processing agreements, ensuring that they deal with data in a manner consistent with the 8 data protection principles
- Advise service managers of their responsibilities with regard to data retention and disposal
- Investigate breaches of the legislation and provide recommendations for improvement
- Advise the Information Commissioner of breaches when appropriate

- Oversee the implementation of the General Data Protection Regulations,

1.5 Change History

Version	Revision Date	Reviser	Previous Version	Description of Revision
1.0	29/06/2001	Mary Gallagher		Original
1.1	19/04/2011	Vikki Smith	1.0	Update format and content
1.2	02/02/2015	Vikki Smith	1.1	Include privacy impact assessments and amend security tips
1.3	03/10/2016	Rosemary Daniel	1.2	DP officer roles & Responsibilities
1.4	12/05/2017	Vikki Smith	1.3	Updates to reflect the GDPR

This manual will be reviewed every three years, or sooner, if there is a significant change.

2. Public Sector Network

The Council is part of the Public Sector Network (PSN), a pan-government network providing a secure network between central government and every local authority in England and Wales. The Council has adopted a number of PSN policies, which will assist in complying with the data protection principles.

PSN secure email is available for all employees who regularly send personal or sensitive customer information and currently use unsecure email, fax, courier or registered postal services to government organisations like the NHS, the Department for Work and Pensions, Criminal Justice Agencies and the Police.

This Manual must be read in conjunction with the following security and information policies:

- **Information Security Incident Management Procedure**
- **Information Risk Policy**
- **Information Handling Practices**
- PSN/GCSx Policies, which can be found on Davnet, under the IT Service Desk page: http://davnet/help-desk/

3. How to use this document

Sections 4 and 5 set out the background to the Regulation and will help you determine whether or not you are processing personal data and therefore need to comply with the Regulation.

Processing of special categories of Personal Data is dealt with in sections 4.3 and 9.

Once you have established that you are dealing with personal data, Sections 5-13 of this document will help you process personal data in accordance with the Regulation.

Sections 14 and 15 deal with the Rights of the Data Subject under the Regulation and what you should do if you receive a request for access to records.

Sections 16 - 18 set out a list of further information points and training aids.

If you have any doubt as to how this manual is pertinent to your role, please read the Data Protection checklist located at **APPENDIX IV**.

4. Overview of the General Data Protection Regulation ("the Regulation")

4.1 Meaning of Personal Data

The Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'. Broadly speaking this means data from which a natural person can be identified and the data relates to that individual.

Due to the nature of the Council's work and the way it holds its information, it should be assumed that any reference to any natural person will constitute personal data and therefore the Regulation will apply. Therefore you can only process the personal data in accordance with the Regulation.

Even if you think that the data that you are dealing with is not personal data for the purposes of the General Data Protection Regulation, the information may still fall within the scope of the Freedom of Information Act. If you are uncertain, please seek legal advice.

4.2 Meaning of 'special categories of personal data'

This is described in the Regulation as "personal data revealing racial, or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

4.3 The Principles

In essence, data protection means that personal data must be processed in accordance with the principles established by the Regulation.

There are **six principles** put in place by the Regulation which specify that personal data must be:

a) processed lawfully, fairly and in a transparent manner

b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) processed in a manner that ensures appropriate security

In addition there is Accountability. The Council is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the ICO.

To demonstrate compliance each Service Area has drafted an Information Asset Register.

5. 'Fair and Lawful' processing

There are other areas of law in relation to the first three Principles that are particularly relevant when considering whether processing is fair and lawful and for a lawful purpose. In particular:-

A. Confidentiality arising from the relationship of the Council employee with the data subject e.g. benefits worker and service user.

B. The ultra vires rule and the rule relating to the excess of delegated powers, under which the Council may only act within the limits of its legal powers.

C. Legitimate expectation - the expectation of the individual as to how the Council will use the information relating to him/her.

D. Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

You should consider whether any of the above applies when you process personal data and seek further legal advice or guidance from your manager.

6. Processing Personal Data

You will be processing personal data if you are carrying out any of the following activities:-

(i) obtaining, recording, holding information
(ii) organising, adapting or using the information
(iii) disclosing or transmitting
(iv) destroying or erasing.

7. Obtaining Personal Data

When obtaining data:-

- Ensure there is legal justification for obtaining personal data. In most cases in your position at the Council, there will be a justification for obtaining the personal data in order for the Council to carry out its functions effectively (such as a statutory purpose)

- If the Council does not have official authority to obtain data, it may be necessary to rely on a different lawful condition, such as a contractual obligation, vital interest or consent.

- DO NOT deceive or mislead the data subject as to the purpose or purposes for which his or her data is to be held, used or disclosed. If you do so you will not have obtained the information fairly or lawfully

- DO NOT request more information than is necessary in order to carry out the specified purpose

- Use the Council's Privacy Notice template to make data subjects aware of their rights and purposes to which their data will be usedFound at **APPENDIX I**

- Ensure that the data obtained is accurate.

7.1 Obtaining information in writing

When obtaining personal information in writing, you must incorporate a Privacy Notice into the form. This notice must be clearly visible and placed appropriately so that the data subject is fully aware of the intended uses of their personal data. Ideally the notice should be provided before personal data is collected.

If consent is required, the Privacy Notice should include this.

A template Privacy Notice can be found at **APPENDIX I.** ***Please note that this is only a template and will need to be tailored accordingly.***

7.2 Obtaining information via the telephone/in person

It is also important that when collecting data via telephone or face to face a Privacy Notice should be made clear to the data subject before any personal data can be obtained.

The Council has a recorded Privacy Notice which is played when the main switchboard number is called. There is a printed version of this notice in the reception.

7.3 Obtaining information from Third Parties

When information is received about a data subject from a third party this information should be provided or be made readily available to that data subject, if he or she requires it, unless this would involve disproportionate effort. Please seek further legal advice or guidance from your manager.

When information is given to the Council about a third party and that party is unaware

that this has happened the Council must notify that third party before using the information.

When information is received from third parties, a statement indicating that the subject's consent has been given to use the information for specific purposes may be necessary.

8. Lawfulness of processing

In order to process personal data you must ensure that you do this in compliance with Article 6, lawfulness of processing, in addition to the data protection principles and other relevant areas of law (see Section 5 above).

The processing of personal data shall only be lawful if and to the extent that at least one of the following applies:

(a) Consent
Consent will not usually be appropriate if there is a clear imbalance of power between you and the individual. This is because those who depend on the Council's services might feel they have no choice but to agree, so consent is not considered freely given.

(b) A contract with the individual
For example to supply goods or services the individual has requested, or to fulfil our obligations under an employment contract. This also includes steps taken at the individual's request before entering into a contract.

(c) Compliance with a legal obligation
If the Council is required by law to process the data for a particular purpose.

(d) Vital interests
You can process personal data if it is necessary to protect someone's life. This could be the life of the data subject or someone else.

(e) A public task
If you need to process personal data to carry out your official functions or a task in the public interest and you have a legal basis for the processing under UK law. As a public authority, this is likely to give the Council a lawful basis for many if not all our activities.

(f) Legitimate interests
Public bodies cannot generally rely on 'legitimate interests'

Consent is not always the most appropriate condition for public authorities to rely on. Therefore the Council is likely to rely on the Public Task condition to carry out official functions or a task in the public interest and not require consent.

8.1 Consent

Consent is described as 'any freely given specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

As referred to in paragraph 7.1 above, the use of the Privacy Notice provides you with an opportunity to obtain consent from the data subject to process their personal information if this is required.

Consider whether the Data Subject has capacity to provide consent. If not, consider whether anyone can provide consent on his or her behalf e.g. someone with power of attorney, of in the case of young children, consent will be from someone with parental responsibility. Children aged 13 and over can provide their own consent.

Ensure that you retain written evidence of consent.

If you cannot obtain consent or you cannot rely on any of the conditions set out in paragraph 8, then you **CANNOT** process the personal information, unless one of the exemptions applies. In such circumstances you should seek legal guidance to see if any of the exemptions are applicable.

9. Consent and special category data

To process this type of data the data subject must give explicit consent. Alternatively **one of the conditions of the following must apply:-**

- The processing is necessary to comply with employment law or social security obligations
- The processing is necessary to protect the vital interests of the data subject (i.e. those affecting life and death) or another person in a case where such consent cannot be given or reasonably obtained or where someone else's interests must be protected and consent has been unreasonably withheld.
- Personal data which are manifestly made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims or wherever courts are acting in their judicial capacity.
- preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or to contract with a health professional
- Protection of the public health
- Substantial public interest

Please seek advice from the Council's Legal Advisor if you wish to rely on consent to process sensitive personal/special category data.

10. Information Sharing

There may be occasions when it is necessary for you to share information with partnership organisations and other professional agencies.

The Department of Education publication '*Information Sharing: Guidance for practitioners and managers*' provides detailed guidance on information sharing. Employees not working with children and young people or vulnerable adults will also find the guidance useful as the principles on sharing personal information are transferable to other areas of work. The guidance can be found at:-
https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

A sharing personal information flowchart can be found at **APPENDIX II**.
The seven golden rules for sharing personal information can be found at **APPENDIX III.**

Information Sharing Agreements

The Council has entered into formal agreements with other organisations which share personal data regularly. We are required to share personal information with other partners and organisations on a regular basis to provide efficient services and also to protect life.

The Information Sharing Agreements are designed to set out the parameters under which this sharing can take place simply, safely and securely.

A register of Information Sharing Agreements can be found on Davnet.

Providing information by telephone

Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the Council. In particular you should:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it (Check your teams local procedure for ID checking).
(b) Suggest that the caller put their request in writing if you are not sure about the caller's identity and where their identity cannot be checked.
(c) Refer to your line manager **OR** Legal Advisor for assistance in difficult situations. No-one should be bullied into disclosing personal information.

When there is no Information Sharing Agreement

There may be occasions when other organisations (such as the Department for Work and Pensions, Home Office, HMRC) request personal information from the Council on an ad-hoc basis and therefore no Information Sharing Protocol will be in place. In these circumstances refer the requester to the Information Officer, who will advise the requester to complete a Section 29 or Section 35 form.

Copies of these forms are available from Davnet.

10.1 Data Protection Impact Assessment

Data Protection Impact Assessments (DPIAs) are a key tool in implementing the "privacy by design" concept and ensure that data protection and privacy are built into new systems and processes from the start. DPIAs help identify the most effective way to comply with data protection obligations and meet individuals' privacy expectations. It aims to identify and fix problems at an early stage.

The ICO recommends that a DPIA looks more broadly at privacy concerns rather than focussing narrowly on data protection compliance.

When should the Council use a DPIA?

Examples include:

- New IT system for storing and accessing personal data
- Data sharing initiative where two or more organisations seek to pool or link a set of personal data
- Using existing personal data held by the Council for a new and unexpected purpose

To determine whether a DPIA is required, you should answer the screening questions referred to the Appendix V.

A DPIA template is available at Appendix VI.

11. Retention and Storage of Data

The Information Handling Practices and the Retention and Disposal Schedules (RDS) can be found on Davnet.

Records should be closed as soon as no longer in use. All closed records held by the Council must have a retention period applied.

Service areas must have procedures in place to check that any data retained or stored is accurate, particularly where the data has not been obtained directly from the data subject.

Subject to statute, Service areas must agree their own retention periods.

Separate periods may be required for data in respect of enquirers and other persons who do not eventually utilise the services of the Council, since these potentially should be retained for more limited periods.

All retention periods that have been agreed should be forwarded to the Information Officer for incorporation in, or updating of, the Retention and Disposal Schedule (RDS).

For further advice on retention of records please contact the Information Officer 01327 302510 or dataprotection@daventrydc.gov.uk.

12. Destruction of Data

The destruction of certain types of records – e.g. financial records – is regulated by Statute. All policies for the disposal of records must comply with Statute and with any guidance from any Government Department. The Council's Retention and Disposal Schedules (RDS) identifies which records are subject to Statute.

13. Security

Detailed policies and procedures on ICT Security can be found on Davnet, under the IT Service Desk page: http://davnet/help-desk/

14. Data Subjects' Rights

The Act gives the following rights to data subjects:

- Right to access their personal information held by the organisation
- Right to rectification of inaccurate personal data
- Right to erasure – does not apply to data processed for the public task
- Right to restriction of processing
- Right to data portability – only where consent is relied upon or where the data subject has entered into a contract with the Council
- Right to object
- Right to prevent significant decisions being taken about them solely by automatic processing

It is important that you are aware, in general terms, of these rights so you know when someone is trying to exercise these. They will not always contain a reference to data protection legislation. You should also know to whom such requests should be referred. In most cases this will be the Information Officer.

Of these rights, that of subject access is the one most likely to be encountered and procedures are required to deal with such requests within the prescribed legal timescale of within one month. In order to prevent complaints to the Information Commissioner you must follow the procedure set out below.

15. Data Subject Access Requests

A subject access request must be made in writing. The Information Officer administers subject access requests.

Subject access requests should be sent to the Information Officer who will log the request, verify the requester's identity and collate the final response. The Information Officer can be contacted by telephone on 01327 302510 or by email: dataprotection@daventrydc.gov.uk

The request will then be directed to the appropriate officer(s) to collate the information. The Information Officer will send a final reply within one month and monitor progress to

be sure it does not exceed the deadline.

16. Reporting Security Breaches/Incidents

The Information Commissioner has the power to impose sanctions in the event of data breach. The Information Commissioner's Office (ICO) is empowered to take the following actions:

- Investigative powers - the ICO has the ability to request information from data controllers and processors, enter and inspect premises, carry out audits and require improvements.
- Civil sanctions - The maximum fine the ICO can issue is up to £17m (€20m) or 4% of global turnover.
- Criminal sanctions - The ICO can prosecute offenders.

In light of the Commissioner's powers it is essential, as soon as you become aware of any data protection incidents, that you report them immediately.

All security incidents, for example a virus infection which could quickly spread and cause data loss or the unintended disclosure of personal or confidential data, must be reported promptly via the ICT Service Desk in accordance with the 'Information Security Incident Management Procedure'. This procedure provides examples of incidents and how they should be managed.

17. Training

E-learning is available via Davlearn. Data protection training is mandatory for employees to complete every two years to ensure their knowledge of Data Protection is up-to-date.

18. Further Information

Data Protection Officer or Information Officer, email: dataprotection@daventrydc.gov.uk

Data Protection Policy http://davnet/strategy-and-policy/

Information Commissioner's Office (ICO): www.ico.org.uk

Government Connect: http://www.govconnect.gov.uk/index.php

Appendix I

Privacy Notices

Example Privacy Notice for self-serve/e-forms /paper forms/ email auto response etc.

Your personal information - what we need and why?
Daventry District Council collects personal information from you in order to deal with your enquiry or service request [WHAT SERVICE?]. This includes your name, address, email etc. We will not collect any personal data from you we do not need. [If you collect more than basic personal information you will need to state what data you collect].

The information you provide will be retained within our [SYSTEM NAME] in order to provide and oversee your service request. It is necessary to hold this data to enable the Council to carry out its public functions.

Who does the Council share your data with?
It may be necessary to share your personal information internally and with [LIST NAMES OF THIRD PARTIES] in order to deal with your service request. However, no other third parties (than the ones listed) have access to your information, unless the law allows them to do so.

How long does the Council keep your data?
The Council is required under [STATE WHICH LAW IS APPROPRIATE] to keep your personal data (name, address, contact details) for a minimum of [X years OR MORE IF APPROPRIATE] after which time it will be destroyed.

What are your rights?
If at any point you believe the information we hold is incorrect you may request to see this information and have it corrected or deleted. If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer who will investigate the matter.

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner's Office (ICO).

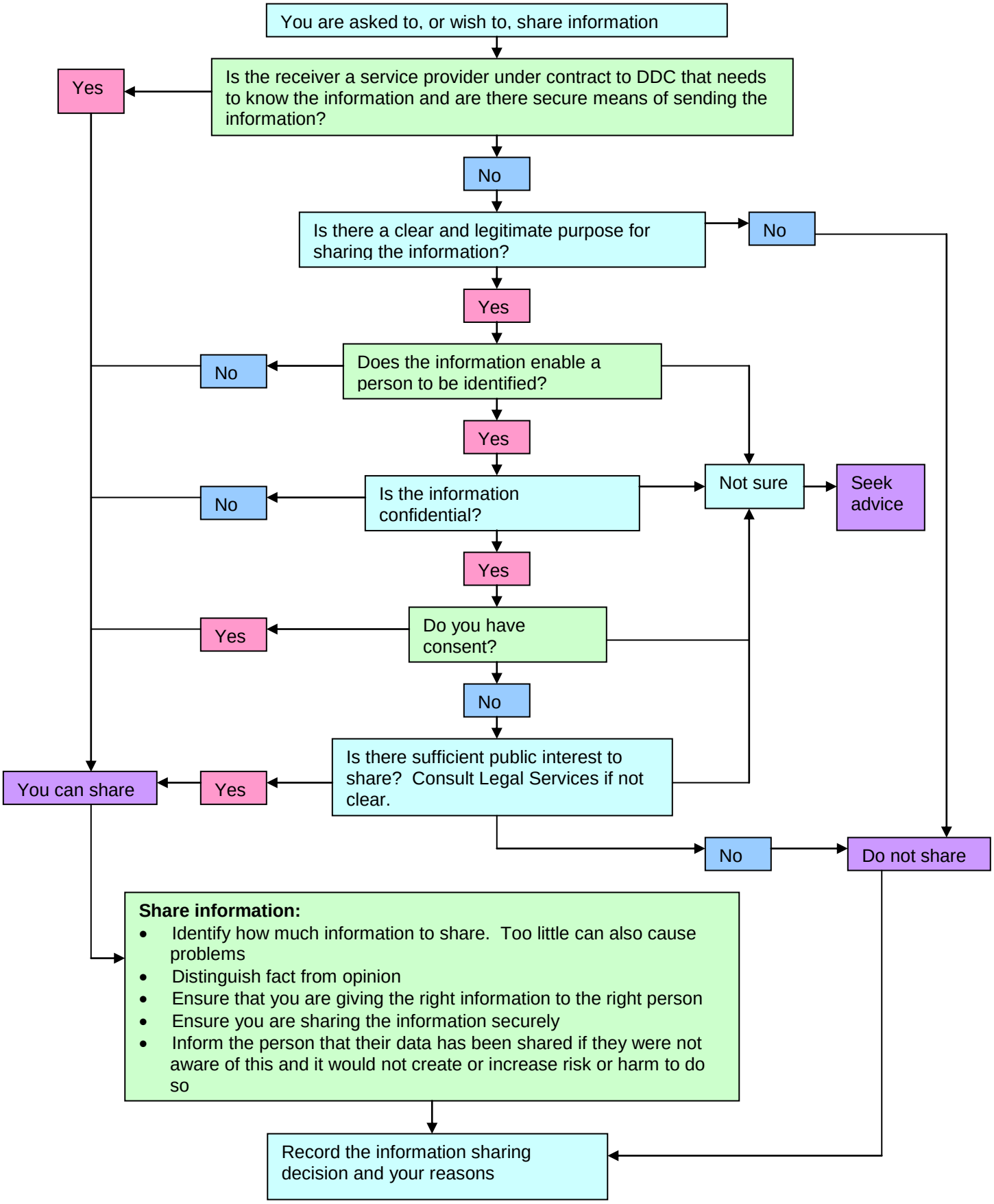
Our Data Protection Officer is Gillian Kennedy and you can contact her by email dataprotection@daventrydc.gov.uk

All information you provide is held in accordance with our Information Charter and in line with the Data Protection Act 2018 and the GDPR. Our Information Charter can be viewed online here www.daventrydc.gov.uk/informationcharter.

NB: these forms will need to be tailored to the purposes for which your service is obtaining information. A "Consent" section should be inserted if consent from the data subject is required. Please contact Legal Services for further advice.

Appendix II

Information Sharing Flowchart



Appendix III

Seven golden rules for sharing information

1. Remember that Data Protection is not a barrier to sharing information but provides a framework to ensure that personal information about an identifiable natural persons is shared appropriately, fairly, lawfully and securely.

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely. If sharing by email, use the confidential flag to encrypt the message.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix IV

Data Protection checklist

If you answer ‘no’ to any of the following questions or you are not sure, you need to read this manual to ensure you are complying with Data Protection legislation.

1) Do I know what I am going to use this information for?

2) Do the people whose information I hold know that I have got it and are likely to understand what it will be used for?

3) If I’m asked to pass on personal information, would the people whose information I hold expect me to do this?

4) Am I satisfied the information is being held securely, whether it’s on paper or on computer?

5) Is access to personal information limited to those who absolutely need to know?

6) Am I sure the personal information is accurate and up to date?

7) Do I delete or destroy personal information as soon as I have no more need for it?

8) Have I undertaken training on my responsibilities under The Data Protection Act and the General Data Protection Regulation (GDPR)?

Appendix V

Do I need to complete a Data Protection Impact Assessment (DPIA)?

Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

1. Will the project involve the collection of new information about individuals?

2. Will the project compel individuals to provide information about themselves?

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition?

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them.

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider particularly private.

8. Will the project require you to contact individuals in ways which they may find intrusive?

Appendix VI

Data Protection Impact Assessment Template

This form should be completed for any existing/proposed policy/function/project where the initial screening questions indicate a significant impact on our customers/employees personal data.

Please answer all questions/complete all sections.

As a result of carrying out an Data Protection Impact Assessment (DPIA), you will have checked that your policy/function/project does not have negative/adverse impacts in terms of personal or sensitive personal relating to customers or employees or if it does you will have identified relevant actions needed to minimise or remove such impact and their likely resource implications.

This is not simply a paper exercise – it is designed to make sure that your policy/function/project and service (development) is delivered fairly to all sections of our local community, and our employees with their privacy in mind.

Please note that this DPIA will be used to support decisions by members and should form part of papers/reports; therefore **your completed questionnaire may become a public document, along with other committee papers.**

The term 'Proposal' will be used throughout the form as a label for what is being assessed – a new policy, new service, new strategy or a change to an existing policy/service/strategy.

1. The Proposal being assessed							
Title of proposal being assessed:							
What type of proposal is this an assessment of?	New Policy/ Strategy	Policy/ Strategy Change	New Service	Change to Service	Service removal	Project	Other
*Put a **x** in the correct box*							
What are the aims and/or objectives of the proposal and the intended outcomes? *If assessing the impact of a proposed change please describe the aims of the change, not the original policy/service*							
Who is intended to benefit from this proposal?							
Who are the main stakeholders in relation to the proposed proposal?							
How is the success of the proposal to be measured?							
Service Area/Team with responsibility for implementation of this proposal							
Name and job title / role of person completing full Screening:							
Date of completion:							

1. Privacy Impact – what are we collecting and how?

1.1	**Is this a new type/s of personal information or information that is already collected?**	New	Old

1.2 What data will be collected?
(Insert basic description here and tick as appropriate below)

Administration data		**Sensitive data**	
Forename		Racial or ethnic origin	
Surname		Political opinion	
Date of Birth		Religious belief	
Age		Trade Union membership	
Gender		Health or Social Care Status	
Address		Sexual life	
Postcode		Commission or alleged commission of an offence	
Unique Identifier (i.e. NI number or similar)		Proceedings for any offence committed or alleged	

Other data *(Please state)*

Will the dataset include health/social care data?	Yes/No
Will the dataset include financial data?	Yes/No

Detailed description of other data collected
If there is any additional feature of the dataset that we should be made aware of please state it here

1.3 How will we collect the data?

Please state by which method the information will be collected?

Email *(Please state whether it is via secure mail (gcsx.gov) or non secure .gov mail)*	
Fax	
Face to face	
Courier	
Web form	
Post (internal)	
Post (external)	
By Hand	
Telephone	
Referral form/other external agency	

Other (please specify)

1.4	**Will the information be collected electronically, on paper or both?**	Electronically	Paper	Both

1.5	**How will individuals be informed about the proposed uses of their personal data?**	*(e.g. privacy notices)*

2. Privacy Impact – how do we use/process/store the data?		
2.1	**Describe in as much detail <u>why</u> this information is being collected/used?**	
2.2	**If consent is not required what is the legal basis for processing this information?**	*(please detail all relevant legislation below)* Choose an item.
2.3	**Where will the information will be stored?**	
2.4	**Is there an ability to audit access to the information?**	Yes/No
2.5	**Does the system/solution involve new links with personal data held in other systems or have existing links been significantly changed?**	Yes/No
2.6	**Will the information be kept up to date and checked for accuracy and completeness (data quality)?**	Yes/No
2.7	**Who will have access to the information?**	*(list individuals or employee groups)*
2.8	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable information?**	
	Username and password	
	Swipe/Access card	
	Key to locked filing cabinet/room	
	2 factor authentication/ Remote Access process	
	Restricted access to Network Files	
	Other: (*Provide a description below)*	
2.9	**Are there any new or additional reporting requirements for this project?**	Yes/No
	Who will be able to run reports?	
	Who will receive the report or where will it be published?	

	Report format:	
	Personally identifiable format?	Yes/No
	Pseudonymised format? De-identify data this means the data is no longer attributed to a specific subject only with additional information	Yes/No
	Anonymised format? Data is not or no longer identifiable	Yes/No

	3. Privacy Impact – how do we share personal data?	
3.1	**Are other organisations involved in processing/using the data?** *(If yes please list)*	Yes/No
3.2	**Does the work involve employing contractors external to the organisation who we would share this information with?** *(If yes please give details)*	Yes/No
3.3	**Will any information be sent offsite – ie outside of the organisation and its computer network (including cloud computing)** *(If yes please give details below including whether you are transferring personal data to a country or territory outside of the EEA?)*	Yes/No
3.4	**Is there an information sharing agreement in place for the above activity?** *(If yes, please provide the location of the agreement and the review date/responsible officer.)*	Yes/No
3.5	**Please state by which method(s) the information is/will be transferred?**	
	Secure Email (if so what type)	
	Fax	
	.GCSX email	
	Courier	
	Website access	
	Post (internal)	
	Post (external)	
	By Hand	
	Telephone	
	Wireless network	
	Other (please specify)	
3.6	**Where appropriate, do we have active consent notices in place for customers/employees to consent for their information to be collected/processed and/or shared?**	Yes/No

4.Privacy Impact – how and when do we archive/dispose of the data collected?		
4.1	**If/when this new/revised function concludes, are there plans in place for how the information will be retained / archived/ transferred or disposed of?** *(If yes, please give details below)*	Yes/No
4.2	**If this information is held in paper records, are they destroyed securely?**	Yes/No
5.Privacy Impact – how do we ensure correct process is followed?		
5.1	**Is Mandatory Employee Training in place for the following?**	Yes/No
	Data Collection (i.e. the process)	
	Use of the System or Service	
	Collecting Consent	
	Data Protection:	
5.2	**Are arrangements in place for recognising and responding to requests for access individuals personal data?**	Yes/No

Please list below an overall assessment of the impact of this proposal and how negative impacts can be minimise and positive ones maximised.

1. **General assessment of impact:**	
a) Does the proposal knowingly prevent us in any way from meeting our statutory equality duties under the Data Protection Act 2018 or General Data Protection Regulations?	*Yes/No*
b) What is the level of impact?	*High/Medium/Low*
c) Summarise the likely negative impacts:	
d) Could you minimise or remove any negative impact that is of low significance?	*How? Brief outline here – more detail on Action plan, below*

Now complete the action planning form below, which will detail the changes that need to be made to this service/policy/function to optimise compliance with our data protection duties.

Data Protection Impact Assessment Action Plan

Action/Risk identified	Key activity	How will we know this has been achieved? (measures, milestones and dates)	Officer responsible	Quarterly progress update

This completed document should be shared with your line manager and with the Data Protection Officer. The Human Rights Implications' section of the report will need to refer to the DPIA to ensure that privacy implications have been taken into consideration when a decision is being made.

Appendix VII

Security Tips

- always use passwords for access to computers and do not share them;
- lock computer screens and log out when you leave the office – even for lunch;
- confirm the identity of callers before discussing service users;
- lock cupboards and filing cabinets containing personal data when not in use;
- control access to keys to cupboards and cabinets;
- control the use and whereabouts of personal computers, especially if they do not belong to the Council;
- do not allow files to be taken home except in controlled circumstances;
- shred documents containing personal/sensitive personal data when they are no longer required;
- emails containing confidential information must be sent via a secure email system; and
- Remember the Golden Rules for handling personal data:
    - Be aware of the personal data around you i.e. in your in-tray, on your desk, on your screen, in letters and emails. Keep desk/screen clear of personal data when unattended
    - Treat this data as though it was your data
    - Only collect, hold and process the data you need
    - Only use it for lawful purposes
    - Update regularly
    - Beware of scammers
    - Ensure data is stored, moved, transmitted and destroyed securely
    - Think privacy - It's in your hands!