Renfrewshire Valuation Joint Board

Report to: **Renfrewshire Valuation Joint Board**

Meeting on: **18th January 2019**

Subject: **Data Protection Policy**

Author: **Data Protection Officer**

1. Introduction

As a result of the General Data Protection Regulations coming into force on 25th May 2018 and the statutory obligation to appoint a Data Protection Officer (DPO), Renfrewshire Valuation Joint Board duly appointed a DPO.

RVJB's DPO has been working with the Assistant Assessor for Governance to ensure RVJB is compliant with the new data protection legislation. One of the outcomes from this partnership working is a new policy governing data protection.

2. Recommendations

i. The Board approve the policy.

Lindsey Hendry
Assistant Assessor & ERO
10th December 2018

For further information please contact Lindsey Hendry at 0141 618 5927 or via email at lindsey.hendry@renfrewshire-vjb.gov.uk.

RENFREWSHIRE VALUATION JOINT BOARD

DATA PROTECTION POLICY

IG1

Title	Data Protection Policy
Author	Heather Syme, Data Protection Officer
Approved By	MTM
Date of Approval	14th November 2018
Reviewer	Assistant Assessor (Governance)
Review Date	Two yearly unless required due to legislative change

Review History

Review No.	Details	Release Date

Contents

1. Introduction

1.1 Renfrewshire Valuation Joint Board (RVJB) is committed to data protection compliance. RVJB expects all employees and elected members to comply fully with this policy and the Data Protection Principles (Appendix 2).

1.2 RVJB needs to collect and use information about people ("Personal Data") to discharge its functions. This Personal Data must be handled properly and lawfully.

1.3 RVJB will hold the minimum personal information necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay.

1.4 Personal information is confidential. Automated systems and relevant filing systems are designed to comply with the Data Protection Principles. Personal information will only be disclosed where necessary.

1.5 It is the responsibility of the Assessor and the Assistant Assessor for Governance to ensure compliance with this Policy. All systems containing information about individuals must be identified, made secure, and notified to the Data Protection Officer for notification purposes. It is the responsibility of all employees to co-operate in this task.

1.6 Upon discovering that this Policy is not being complied with, the Clerk after consultation with the Treasurer of the Board, shall have full authority to take such immediate steps as considered necessary.

1.7 Although data protection legislation is complex, its ethos is simple. It protects people's Personal Data by regulating the way in which organisations, such as RVJB, handle information.

1.8 The Data Protection Act 1998 ("DPA") has imposed obligations on RVJB, as a data controller, since 1 March 2000. However, as of 25 May 2018, the EU General Data Protection Regulation ("GDPR") is in force.

1.9 It is impossible to understand data protection without an awareness of some of the key definitions. Some definitions in GDPR are slightly different to those in the DPA. These are as follows:

"Controller", previously known as "Data Controller" means the organisation who determines the purposes and means of processing.

"Processor", previously known as "Data Processor" is anyone, other than an employee of the controller, who processes Personal Data on the data controller's behalf.

"**Processing**" still covers anything which can be done with Personal Data, from simply collecting or storing, recording, altering, to actively disclosing this and includes verbal, as well as written exchanges, information left on desks or in confidential waste bags.

"**Personal Data**" is information relating to a living individual who can be identified directly or indirectly from this. This means that even just an address can be Personal Data if it can indirectly identify someone.

"**Special Category Data**" is an additional category of personal data, replacing "Sensitive Personal Data" and includes information on racial or ethnic origin, religion, political opinions, religious beliefs, details of physical or mental health or condition, sexual life or details of any offence. Like sensitive personal data and the DPA, there are some stricter rules in the GDPR for lawful processing of Special Category Data.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

1.10 The Data Protection Principles

Under GDPR there are six Data Protection principles which cover rules for the maintenance, collection and security of personal data. RVJB is committed to complying with the Data Protection Principles.

As such, RVJB undertakes that Personal Data will:

1. Be processed fairly and lawfully and transparently.
2. Be collected and processed only for one or more specified, explicit and legitimate purpose(s).
3. Be adequate, relevant and limited to what is necessary.
4. Be accurate and kept up to date and that inaccurate data will be erased or rectified without delay.
5. Be kept for no longer than is necessary.
6. Be processed with appropriate security and use adequate technical and organisational measures to prevent unauthorised or unlawful processing or accidental loss, destruction of, or damage to Personal Data.

In addition, under GDPR, RVJB now needs to be able to demonstrate compliance with the principles. This is referred to as “accountability”.

2. Scope

This policy applies to all employees of RVJB and covers all Personal Data and Special Category Data which they process. It may, however, be read alongside other RVJB policies and guidelines on use of non-personal data and wider information governance issues.

3. Data Protection Governance Arrangements

3.1 RVJB has a corporate responsibility for data protection and is defined as a “Controller” under GDPR.

3.2 The GDPR obliges RVJB to designate a statutory Data Protection Officer (DPO) on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

3.3 The key tasks of the DPO are prescribed and are to:

- Inform and advise RVJB on GDPR compliance;
- Monitor compliance;
- Advise on Data Protection Impact Assessments;
- Train staff;
- Conduct internal audits;
- Be the first point of contact for the regulator; and
- Have due regard to the risk associated with RVJB's processing operations.

3.3 All employees are individually responsible for ensuring that the processing of Personal Data is in accordance with GDPR and should familiarise themselves and comply with RVJB data protection guidance. Advice can be obtained at any time from the Data Protection Officer.

3.4 The Data Protection Officer will offer ad hoc advice on data protection issues.

3.5 The Data Protection Officer has a key role in ensuring compliance with the sixth principle relating to data security by providing advice and guidance to Services on information security, maintaining RVJB's Information Security log and leading on information security incident management.

4. Notification

GDPR removes the requirement in the Data Protection Act to notify the Information Commissioner's Office (ICO) of all Data Controllers. However, a provision in the Digital Economy Act means that Controllers still need to pay the ICO a fee, dependent on the size of the organisation. The ICO has produced guidance on the new fee structure, which was laid before Parliament at the end of February 2018.

5. Documentation of Processing Activities

Although there is no longer a notification requirement, Controllers are obliged to document their processing activities under GDPR. There are some similarities between this new obligation and the information previously provided to the ICO for notification. RVJB's notification and the Information Asset Register will form the basis of RVJB's documentation of processing activities. This contains details of RVJB's information assets, how those were obtained, how they are being used and who they are shared with.

6. Data Subject Rights

6.1 Data subjects have several significant rights under GDPR, which are as follows:

- Right to be informed;
- Right of access;
- Right to rectification of inaccurate data;
- Right to erasure in certain circumstances;
- Right to object to certain processing, including the right to prevent processing for direct marketing;
- Right to prevent automated decision-making;
- Right to data portability and
- Right to claim compensation for damages caused by a breach.

6.2 The right most frequently used by RVJB service users is likely to be the right of access, i.e. the right of an individual to access his/her own Personal Data. Under GDPR, RVJB has one a maximum of one calendar month (instead of 40 calendar days) to comply with subject access requests. The maximum £10 fee which was chargeable under the DPA has been abolished by GDPR and so, this is now free of charge.

Further information on compliance with all data subject rights, particularly subject access rights, can be obtained from the Data Protection Officer.

7. Training and Guidance

The Data Protection Officer will continue to prepare and revise detailed guidelines on the practicalities of dealing with GDPR.

8. Data Retention

8.1 The fifth data principle states that Personal Data should not be held for longer than is necessary. What is necessary can vary, depending on the nature of the information and why it is held. Each employee has a responsibility to ensure that appropriate retention schedules are in place for records which they hold, and to arrange for the secure destruction of data, in accordance with such schedules.

8.3 In accordance with its obligations under the Public Records (Scotland) Act 2011, RVJB has adopted a Records Management Plan containing appropriate retention and disposal schedules. This will ensure compliance with the fifth data protection principle.

9. Information Security

9.1 The sixth data protection principle provides that appropriate technical and organisational measures should be taken to ensure that all Personal Data is secure.

9.2 All employees have responsibility for keeping the Personal Data to which they have access to safe and secure.

9.3 By adopting recognised information security practices, RVJB can demonstrate, to customers, partners and stakeholders that it can be trusted to protect the confidentiality, integrity and accessibility of the information it holds.

9.4 Information Security is not purely a technical issue. Information security principles apply to all information held by RVJB, whether this is held in electronic or non-electronic format, even extending to conversations between individuals.

9.5 Employees who become aware of a potential breach of information security, such as a loss of data, must immediately report this to the Data Protection Officer, in line with the Information Security Incident Reporting Procedures.

9.6 Further information and advice on information security can be obtained from the Data Protection Officer at any time.

10. Data Processors

If someone, other than an employee of RVJB, is processing Personal Data on its behalf, for example, a contractor, RVJB, as Controller, is obliged to have a written agreement with the Processor. Further information on Data Processor Agreements can be obtained from the Data Protection Officer.

11. Information Sharing

Although processing of Personal Data must always be fair and lawful, data protection should not be perceived as a barrier to effective inter-agency information sharing. There are many situations where information can, and indeed, must be shared, for example, to protect individuals. Advice on information sharing can be obtained at any time from the Data Protection Officer. Consideration should, however, be given to the following:

- What information needs to be shared?
- With whom?
- Why?
- How?
- What are the risks of not sharing the information?
- Could the same aim be achieved without sharing the data or by anonymising it?

12. Data Protection Impact Assessments (DPIAs)

12.1 DPIAs are carried out for any new initiatives or changes of business practice involving Personal Data. Its purpose is to:

- Identify any potential and likely impact on privacy; and
- Minimise and manage the identified impact and privacy risks.

12.3 Under GDPR, DPIAs replace PIAs and makes them mandatory, rather than just good practice. This is a process which enables RVJB to address the potential privacy risk and impact from the collection, use and disclosure of Personal Data as a result of new initiatives and to ensure means are in place to make sure data protection compliance and privacy concerns are addressed appropriately.

12.2 Advice on and assistance with carrying out DPIAs can be obtained from the Data Protection Officer.

13. Relationship with Other Legislation

13.1 Human Rights Act 1998

Public authorities, such as RVJB, must comply with the Human Rights Act 1998 ("HRA") in the performance of their functions. Section 6 HRA obliges public authorities to act in a manner which is compatible with the rights contained in the European Convention of Human Rights ("ECHR"). Article 8 ECHR affords everyone the right to respect for private and family life, including home and correspondence. Although this right is not absolute, any interference must be justified on the basis that it is lawful, necessary to pursue a legitimate aim and proportionate. This means that the interference should not be greater than is necessary to achieve the legitimate aim.

HRA is therefore a consideration when considering whether there is a justification for sharing information. Whilst data protection compliance may render an interference lawful, RVJB must also consider whether information sharing exercises are necessary in the public interest or whether the same ends can be achieved by a less intrusive means before an interference with Article 8 privacy rights can be justified. If there is a less intrusive alternative, the interference will be disproportionate.

13.2 Freedom of Information (Scotland) Act 2002

The interface between the data protection and the Freedom of Information (Scotland) Act 2002 ("FOISA") is complex. FOISA obliges RVJB to be open and transparent, whereas data protection and HRA protect people's information and personal privacy. Although FOISA provides the public with a right of access to all information held, unless this is covered by one of a number of fairly narrow exemptions, there is an absolute exemption from disclosure for information, disclosure of which would breach the data protection principles. Further information on the Personal Data exemption under FOISA and how to deal with freedom of information requests without breaching data protection can be obtained at any time from the Data Protection Officer.

14. Breach

14.1 Breach of this policy may be regarded as a serious act of misconduct and may lead to disciplinary action. Employees must therefore make every effort to ensure that they understand their responsibilities under this policy.

14.2 It is a criminal offence under the GDPR to knowingly or recklessly obtain, disclose or procure Personal Data without the consent of the Controller. RVJB reserves the right to report any such offence to the Police, as well as the Information Commissioner.

15. Audit

Data protection procedures are subject to routine internal and external audit and recommendations implemented accordingly.

16. Review

This policy will be reviewed on a two-yearly basis, unless earlier review is required due to legislative changes. However, to ensure ongoing data protection compliance, any developments, significant cases, guidance from the ICO, or other lessons learned in this area, will be used to inform best practice.

APPENDIX 1: DATA PROTECTION OFFICER

Heather Syme, Senior Solicitor (Information Governance)

Renfrewshire Council

Heather.syme@renfrewshire.gov.uk

Tel: 0141 618 7022

APPENDIX 2: THE DATA PROTECTION PRINCIPLES

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

Why are the principles important?

The principles lie at the heart of the GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don’t give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to compliance with the detailed provisions of the GPDR.

Failure to comply with the principles may leave RVJB open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

APPENDIX 3: SAR GUIDELINES

These guidelines explain the rights of individuals to access their personal data.

Key points

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

What is an individual entitled to?

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information (this largely corresponds to the information that is in the Privacy Notice).

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data.

Other information

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;

- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to you verbally or in writing. It can also be made to any part of your organisation (including by social media) and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.

This presents a challenge as any RVJB employee could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. It is also recommended that you keep a log of verbal requests.

How should we provide the data to individuals?

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

We have received a request but need to amend the data before sending out the response. Should we send out the “old” version?

A subject access request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So, it would be reasonable for you to supply information you hold when you send out a response, even if this is different to that held when you received the request.

However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

Do we have to explain the contents of the information we send to the individual?

The GDPR requires that the information you provide to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child.

At its most basic, this means that the additional information you provide in response to a request should be capable of being understood by the average person (or child). However, you are not required to ensure that that the information is provided in a form that can be understood by the particular individual making the request.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a subject access request.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a “reasonable fee” for the administrative costs of complying with the request. You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.

How long do we have to comply?

You must act on the subject access request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

What about requests for large amounts of personal data?

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.

You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding

to the request begins when you receive the additional information. However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

What about requests made on behalf of others?

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters (e.g. the Sheriff Court).

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;

- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown.

What should we do if the data includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

If we use a processor, does this mean they would have to deal with any subject access requests we receive?

Responsibility for complying with a subject access request lies with you as the controller. You need to ensure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of

whether they are sent to you or to the processor. More information about contracts and liabilities between controllers and processors can be found here.

You are not able to extend the one-month time limit on the basis that you have to rely on a processor to provide the information that you need to respond.

Can we refuse to comply with a request?

You can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.
- In either case you need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

What should we do if we refuse to comply with a request?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

Can I require an individual to make a subject access request?

In the DPA 2018 it is a criminal offence, in certain circumstances and in relation to certain information, to require an individual to make a subject access request. We will provide further guidance on this offence in due course.

APPENDIX 4: DATA PROTECTION IMPACT ASSESSMENTS

What are they and when are they needed?

A DPIA should be considered for any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

It is designed to identify any privacy risks and ensure that those risks are minimised while still allowing the aims of the project to be met.

A DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The Data Protection Officer will work with you to discuss your project and what (if anything) needs to be done to reduce the risks to people's privacy.

Examples of where a DPIA would be helpful:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of RVJB.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.

Key points

- A DPIA will help to identify and minimise the privacy risks of new projects or policies.
- Conducting a DPIA simply involves working with the Data Protection Officer to identify and reduce privacy risks.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Contact the Data Protection Officer for more information on DPIAs or to talk through whether it might be helpful to carry out a DPIA before you embark on a new project or policy which could have an impact on the way you use personal information.