Runnymede Borough Council

Data Protection Policy

January 2024

Classification	Official	
Version	1.9	
Author	Data Protection Officer	September 2018
Owner	Data Protection Officer	
Reviewed by	IT; Information Governance	
Approved by	CLT	05/02/2019
Distributed to	Staff pages; Website	
Linked Policies	Code of Conduct;	

Review date	Changes	Version
January 2019	Minor amendments	1.5
July 2021	Added NHS opt-out and updated legislation references	1.6
August 2023	Updated section 2.4	1.7
November 2023	Updated links	1.8
January 2024	New format	1.9

Contents

1. Overview

1.1 Runnymede Council is committed to ensuring the privacy of individuals is respected and that all personal data that is processed by the organisation is dealt with in accordance with the requirements of the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other related legislation.

1.2 The GDPR lays down rules relating to the protection of natural persons regarding the processing and sharing of personal data; it protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

1.3 The Council will therefore aim to ensure that all employees, elected members, contractors, agents, consultants, or partners of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the law. Specifically in respect of:

- their responsibilities under data protection law for the protection of personal data
- the necessity of appropriate data sharing
- the benefits for good records management
- the technical and administrative controls operating at the council.

1.4 This policy should not be read in isolation and regard should be given to the Information Technology policies, Information Governance Framework, and relevant Code of Conduct.

1.5 Any queries about your data protection obligations or the rights of individuals should be directed to the Data Protection Officer or the Information Governance Officer.

2. The Law and Definitions

2.1 Summary

2.1.1 The UK Data Protection Act 2018 (DPA) and UK General Data Protection Regulation 2021 (GDPR) governs how personal data should be processed. It also gives rights to individuals whose data is held. The UK GDPR came into force on 1 January 2021, when the EU GDPR was enshrined in UK law. It applies to all personal data collected whether held on computer or manual record (if it is intended to form a part of a filing system). The law is enforced by the Information Commissioner's Office (ICO).

2.1.2 From this point forward unless specifically stated reference to 'GDPR' will also include the Data Protection Act 2018.

2.1.3 Under GDPR data is owned by the data subject. This means we are only the custodians and must ensure we safeguard the data.

2.2 Personal data

2.2.1 The definition of personal data is broad. It is defined as any information relating to an identified or identifiable living individual, where an "Identifiable living individual" means you can distinguish them from other individuals, directly or indirectly, in particular by reference to:

a) an identifier such as a name, an identification number, location data or an online identifier (e.g. IP addresses and cookie identifiers) or

b) one or more factors specific to that individual.

2.2.2 Whether a potential identifier distinguishes an individual depends on the context. You do not have to know someone's name for them to be identifiable, a combination of identifiers may be sufficient to distinguish them from other individuals and therefore identify them.

2.2.3 You may not be able to directly identify an individual from the information you possess, however you also need to consider what other sources of information could be available, both internally and externally, which could identify an individual if put together with the information you hold.

2.2.4 In order for the information to be personal data it also needs to 'relate to' that identifiable individual. It is not sufficient that the information merely distinguishes them from others; it must also concern the individual in some way.

2.2.5 To decide whether or not data relates to an individual, you may need to consider:

- the content of the data – is it directly about the individual or their activities?
- the purpose you will process the data for; and
- whether processing the data will have an impact on the individual.

2.2.6 The **Data Subject** is the identified or identifiable living individual to whom personal data relates.

2.2.7 It will not always be clear whether the information is personal data. If this is the case, you should contact the Data Protection Officer for advice. Furthermore, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

2.3 Special category 'Sensitive' personal data

2.3.1 GDPR makes a distinction between personal data and special category "sensitive" personal data. Special category personal data is subject to stricter conditions of processing.

2.3.2 Special category data is defined as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

2.4 Criminal proceedings or convictions

2.4.1 As part of the Council's statutory functions, we can investigate and prosecute individuals and organisations for certain offences. Where personal data is processing for this reason, we will be processing the data under Part 3 of The Data Protection

Act 2018. Please see our Law Enforcement Appropriate Policy Document for further details.

2.4.2 Any other processing of data relating to criminal convictions and offences, or related security measures is dealt with in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.

2.5 Processing

2.5.1 Processing in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

(a) collection, recording, organisation, structuring or storage

(b) adaptation or alteration

(c) retrieval, consultation or use

(d) disclosure by transmission, dissemination or otherwise making available

(e) alignment or combination, or

(f) restriction, erasure or destruction

2.5.2 It should be noted that you are still processing personal data even if the information was not sent at your request.

2.6 Data Controllers and Data Processors

2.6.1 **Data Controller** determines the purposes and means of processing personal data.

2.6.2 **Joint Data Controller** determines the purposes and means of processing personal data jointly with another data controller.

2.6.3 **Data Processor** is responsible for processing personal data on behalf of a controller under their specific instructions.

2.6.4 GDPR puts obligations on both data controllers and processors to maintain records of personal data and processing activities and they may be held responsible for a data breach.

2.6.5 There are also obligations on data controllers to ensure contracts with processors comply with GDPR principles.

3. Data Protection Principles

3.1 Overview

3.1.1 The GDPR (Article 5) contains 7 principles for processing personal data with which organisations must comply. The **data protection principles** require that personal data shall be:

3.1.2 processed lawfully, fairly and in a transparent manner **('lawfulness, fairness and transparency'**)

3.1.3 collected for specified reason and not used for another unrelated reason **(‘purpose limitation’);**

3.1.4 collected only where necessary for the identified purpose **('data minimisation')**

3.1.5 accurate and, where necessary, kept up to date; **('accuracy')**

3.1.6 kept as long as necessary for the purposes for which the personal data is processed and no longer. **('storage limitation')**

3.1.7 processed to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using relevant IT security methods or organisational policies and procedures **('integrity and confidentiality').**

3.1.8 As a controller we are responsible for, and must be able to demonstrate compliance with, the above data protection principles. There is an additional principle known as **'accountability'** which specifies this requirement**.**

3.2 Lawful basis for processing

3.2.1 In order for the processing to be lawful, you must not be breaking the law by processing the information AND there must be a 'lawful basis' for processing.

3.2.2 To comply with a lawful basis for processing information, the processing must be necessary. This requires a targeted and proportionate way of achieving the purpose, and compliance with for one of the following lawful basis:

(a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. Consent must be freely given, and you cannot use this lawful basis if there is an imbalance of power in your relationship with the data subject. For example, if you are processing in the capacity of the Local Authority or an employer and not consenting would be detrimental to the data subject.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This lawful basis cannot apply if you are a public authority processing data to perform your official tasks.)

3.2.3 Special category information requires at least one further condition to be satisfied. Processing of special category data cannot occur unless one of the following applies:

(a) the data subject has given **explicit consent**. Explicit consent must be expressly confirmed in words. Individuals do not have to write the consent statement in their own words; you can write it for them. However, you need to make sure that the data subjects can clearly indicate that they agree to the statement – for example by signing their name or ticking a box next to it.

(b) processing is necessary for **employment, social security and social protection law**.

(c) processing is necessary to protect the **vital interests** of any individual where the data subject is incapable of giving consent. You cannot use this lawful basis in advance of an emergency if the data subject has the capability give consent.

(d) processing for the legitimate interests of a foundation, association or any other **not for profit body with a political, philosophical religious or trade union aim**.

(e) information has already been **made public** by the data subject

(f) processing is necessary for the establishment, exercise or defence of **legal claims** or court action

(g) necessary for reasons of **substantial public interest**, such as;

i) employment, social security and social protection

ii) health and social care purposes

iii) research

iv) statutory government purposes

v) equality of opportunity or treatment

vi) racial and ethnic diversity at senior levels of organisations

vii) preventing or detecting unlawful acts

viii) protecting the public against dishonesty and preventing fraud

viiii) support for individuals with a disability or medical condition

x) safeguarding of children and of individuals at risk

xi) information provided to elected representatives

Please note this is not an exhaustive list and the Data Protection Officer should be consulted for further information.

(h) preventative or occupational medicine

(i) public health

(j) archiving and research

3.3 Fairness and transparency

3.3.1 To comply with the fairness aspect of this principle you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

3.3.2 To be transparent you must be clear, open and honest with people from the start about how you will use their personal data.

3.3.3 Providing access to a Privacy Notice helps ensure that the fairness and transparency aspects of this principle are complied with. Please see the individual's right to be informed for further details.

3.4 Data Quality, Integrity and Retention

3.4.1 Personal data held should be directly relevant to the reason the information was collected and not excessive.

3.4.2 You will ensure, as far as is practicable, that the information held is accurate and up to date. If personal data is found to be inaccurate, this will be remedied as soon as possible.

3.4.3 You will adhere to the council's **Information Governance Framework** which provides a guide on achieving data quality standard for the Council.

3.4.4 Personal information, such as contact details, may be shared within the Council where it is necessary to keep records accurate and up-to-date, and to provide individuals with a better service.

3.4.5 Records may include professional opinions about individuals, but employees should not record any personal opinions about individuals.

3.4.6 The Council's use of personal data will comply with the **Corporate Retention Schedule** and specific retention periods will be listed in departmental **Record of Processing Activities** on the council's X:drive.

3.4.7 Information will only be held for as long as is necessary after which the details will normally be deleted or fully anonymised so that the individual cannot be identified. Where details of individuals are stored for long-term archive or historical reasons, it will be done within the requirements of the legislation.

3.4.8 Redundant personal data will be destroyed using the Council's procedure for disposal of confidential waste and in accordance with departmental retention schedules. This requires all paper-based documents to be shredded or disposed of in confidential waste bins located in the council offices.

3.5 Security and data breaches

3.5.1 Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with Information security arrangements and policies, including the obligation to report a data breach may result in disciplinary action, including dismissal.

3.5.2 The Council will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.

3.5.3 An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access will not be tolerated.

3.5.4 The Council has a Data and Cyber Security Policy and an Acceptable Usage Policy which applies to electronic systems containing personal data. All Information Security Incidents should be dealt with in line with the Incident Management Policy and reported to Digital Services (digital.services@runnymede.gov.uk) and the Data Protection Officer (dpo@runnymede.gov.uk)

3.5.5 All other personal data breaches, however minor, should be reported by emailing dpo@runnymede.gov.uk. This should be done as you become aware of the breach or suspected breach, even if you are not sure of all the facts. This email address will be monitored by the Data Protection Officer, the Information Governance Officer, and the Head of Law and Governance.

3.5.6 A personal data breach which is likely to result in a risk impacting the data subjects control or privacy over their data must be reported by the Council to the Information Commissioner's Office (ICO) no later than 72 hours from the point the council becomes aware of the breach.

3.5.7 A personal data breach which is likely to result in a *high* risk to the individuals must be reported to the impacted individuals without undue delay.

3.5.8 Employees are obliged to report any data breaches they become aware of. Harassment towards employees who have reported data breaches will not be tolerated and will be dealt with in accordance with the Council's Whistleblowing policy.

3.5.9 All managers and staff within the Council's departments will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

3.5.10 Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

3.5.11 Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices or media.

3.5.12 Security arrangements will be reviewed regularly by Digital Services, any reported breaches or potential weaknesses will be investigated in line with the Incident Management Policy and, where necessary, further or alternative measures will be introduced to secure the data.

3.5.13 Employees who process personal data out of the office (e.g. off site, on client premises, at home) can only do this with the express approval of their senior manager. Access to personal data outside of the Council should not be attempted using unsecured access systems, including sending personal data to an employee's personal email account.

3.5.14 Where it is necessary to leave documents containing personal data for a short time i.e. whilst on a site visit, the documents should be kept out of sight and in a secure location e.g. the boot of a locked car. As soon as the documents can be moved to a more secure location such as the office or the officer's home address this should be done.

3.5.15 Any documentation containing personal data should be returned to the council to be put into confidential waste bins or shredded. Under no circumstance should Council documentation be disposed at an employee's personal address.

3.5.16 When an employee is working off-site, they must ensure that personal data is not viewed or accessed by any members of their family or visitors to their household.

3.5.17 Personal data will not be transferred outside the European Economic Area without the approval of the Data Protection Officer and Head of Law and Governance. This includes using data processors to store or host data outside the EU.

3.6 Accountability and Documentation

3.6.1 As a data controller, the Council is responsible for compliance with the data protection principles. There is an explicit requirement for us to be able to demonstrate this. We need to be proactive about data protection, and evidence the steps we take to meet our obligations and protect people's rights.

3.6.2 Contracts between the council and our processors ensure that we both understand our obligations, responsibilities and liabilities. They help processors to comply with the GDPR, and the Council to demonstrate our compliance with the GDPR. Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller**.**

Contracts must also include as a minimum, the following terms, requiring the processor to:

- only act on the written instructions of the controller.
- ensure that people processing the data are subject to a duty of confidence.
- take appropriate measures to ensure the security of processing.
- only engage sub-processors with the prior consent of the controller and under a written contract.
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

3.6.3 Information Sharing Agreement (ISA) is appropriate where systematic sharing of personal data occurs without a contract in place. This is usually applicable where two data controllers are sharing data for a specified purpose, for example sharing data between local authorities or NHS. The agreement should broadly cover the same categories as stated in 3.6.2. Copies of the ISA should be retained by the service and also sent to the Data Protection Officer to keep a central record of all ISAs.

3.6.4 Record of Processing Activities (Article 30) lists specific information that we are obliged to record. This enables a solid documented understanding of the purposes and legal basis of data processing across all Council departments. The law prescribes the following needs to be recorded for each processing purpose.

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer.
- the purposes of the processing.

- a description of the categories of data subjects and of the categories of personal data.
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- where applicable, transfers of personal data to a third country or an international organisation.
- the envisaged time limits for erasure of the different categories of data.
- a general description of the technical and organisational security measures.

3.6.5 A Data Protection Impact Assessment (DPIA) is an essential accountability tool and a key part of taking a data protection by design / default approach to what we do. It helps us to identify and minimise the data protection risks of any new projects we undertake which involve or have an impact on personal data.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests, such as processing involving the following.

- Automated decisions
- Health
- CCTV
- Children
- Biometric/genetic data

However, DPIA screening questions should be completed prior any new project or change to existing procedures. The screening questions will indicate whether a full scale DPIA is required. Please see the **DPIA form** for further guidance.

4 Rights of individuals

4.1 Right to be informed / Privacy Information

4.1.1 Individuals have the right to be informed about the collection and use of their personal data at the time their information is collected. Also known as a **Privacy Notice**.

4.1.2 If you have not received the information directly from the data subject then you must provide the Privacy Notice within a month of receiving the information or when you first communicate with the data subject or share their information with a third party, if this is sooner.

4.1.3 Privacy Notice needs to include:

(a) the name and contact details of the organisation and their DPO

(b) the purposes of processing

(c) the lawful basis of processing including an explanation of the legitimate interests if processing under this lawful basis

(d) the categories of personal data collected

(e) who the information may be shared with, including any transfer of data outside the EU

(f) the relevant retention period

(g) the data subject's rights

(h) how to make a complaint

4.1.4 There are a few circumstances where privacy information does not need to be provided, such as.

(i) if an individual already has the information

(ii) it would involve a disproportionate effort to provide it to them

4.1.5 The overarching Council Privacy Notice is located on the Council website under 'Privacy Statement'. Relevant departmental Privacy Notices are also linked from this page. You should ensure that when personal data is collected you provide the data subject with a Privacy Notice either via a link or in hardcopy. To ensure that the information is easily accessible you may want to include the link in your email signature.

4.1.6 When we collect personal data, we need to be specific about the reasons why. Whenever you are collecting personal data, for example in a form, please provide an explanation of why the information is being collected and what will happen with their data including any sharing that is envisioned. You should also link to your broader departmental privacy notice on the webpage. Further guidance on what should be included is available in the **'How to provide privacy information when collecting personal data in a form'**

4.2 Right of Access / Subject Access

4.2.1 Individuals have the right to access their personal data. This is commonly referred to as **subject access**. It gives individuals the right to obtain a copy of their personal data as well as the privacy information i.e. the purposes of processing, who the information has been shared with etc. This helps individuals to understand how and why we are using their data, and check we are doing it lawfully.

4.2.2 The requests can be made verbally or in writing. The request does not need to specify subject access, data protection etc. if it is clear they are requesting their own personal data.

4.2.3 Subject access requests are coordinated and monitored by the Information Governance Officer. If you are made aware of a request, please notify the Information Governance Officer as soon as possible using foi@runnymede.gov.uk..

4.2.3 You have one month to respond to the request, but this can be extended by a further two months if the request is complex or you have received several requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary. However please liaise with the Information Governance Officer prior to making this decision.

4.2.4 If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise. This could mean where it is not possible to provide an electronic copy you must provide access to the information on your live system. This will need to be monitored closely.

4.2.5 Although no fee is applicable when making the request the law does allow you to charge a "reasonable fee" for the administrative costs of complying with the request where the request is manifestly unfounded or excessive. 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. Please contact the Information Governance Officer if you think a charge is appropriate.

4.2.6 In order to establish the identity of the requester it may be appropriate to request identification. This will apply where you do not have an ongoing relationship with the requester. In this case at a minimum, you should request a copy of a photo ID such as a driving licence or passport and proof of address such as a utility bill. 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.

4.2.7 If the request is very broad you can ask the requester to be specific about the department or nature of the information they want. However, you cannot limit the scope of their request. If they refuse, then you should undertake the search based on your best efforts to locate the information. If you request clarification the period for responding begins once a response is received.

4.2.8 An individual can make a subject access request on behalf of a third party. For example, a parent on behalf of their child or a solicitor on behalf of their client. However, they need to provide evidence of their authority to make the request.

4.2.9 If a child is under 13 the parent can make the request on their behalf but must provide proof of parental responsibility i.e. a copy of their birth certificate which names them as a parent. If the child is over 13 the parent would need to get their child's consent.

4.2.10 If you have concerns that the data subject is neither aware nor wants the third party to access the information that will be disclosed as a result of the request you can send the data directly to the data subject. Where the information relates to health, social care or child abuse data you can withhold the information if it is not appropriate to send directly to the data subject. Please contact the Information Governance Officer who can advise you further.

4.2.11 For further information on how to comply with a subject access requests can be found on the staff pages under **Subject Access Requests**.

4.3 Right to rectification

4.3.1 Data subjects have the right to have inaccurate personal data rectified or incomplete data completed. This is closely linked to the obligation to keep records up to date (3.1.5). However, this right requires us to reconsider the accuracy of our records when specifically requested.

4.3.2 A data subject may disagree with an opinion but that does not mean it is inaccurate as it will be a true reflection of an individual's opinion at that time. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, depending on the circumstances it will not be considered inaccurate and does not need to be rectified. However, a note can be placed on file stating that the data subject disputes the opinion.

4.3.3 Whilst you are considering the accuracy of the data it is good practice to restrict further processing until a determination can be made.

4.3.4 If it is determined that the information is inaccurate you should update the information as soon as possible and notify the data subject of your action.

4.3.5 In some cases it may be important to keep a record of the mistake. In such circumstances the fact that a mistake was made, and the corrected information should also be included in the individual's data.

4.3.6 If it is determined that the information is accurate you should notify the data subject, within one month of receiving the request, of the reasoning behind the decision, inform them of their right to complain to the ICO and their ability to seek to enforce this right through a judicial remedy. Please also notify the Council's Data Protection Officer if you are intending to refuse a request for rectification.

4.4 Right to erasure

4.4.1 Data subjects have the right to have personal data erased. This is also known as the 'right to be forgotten'. This right applies in the following circumstances.

- The information is no longer necessary for the purposes you collected it
- You are processing the information based on consent and the data subject has now withdrawn their consent.
- You are processing the information based on legitimate interests and the data subject objects, where no overriding legitimate interest exists.
- You have breached the first data protection principle (3.1.2) and are processing unlawfully.
- There is a legal obligation to erase the data.
- The processing of data is for the purpose of offering information society services to a child.

4.4.2 If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

4.4.3 As well as your live systems you will have to take steps to ensure erasure from backup systems. Those steps will depend on your particular circumstances, your retention schedule (particularly in the context of its backups), and the technical mechanisms that are available to you. For example, it may be that the information is erased from the live system instantly but the backup system will need to wait until it is overwritten. The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten.

4.4.4 The right to erasure does not apply in the following circumstances.

- Processing is necessary to exercise the right of freedom of expression and information.
- Processing is necessary to comply with a legal obligation.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Processing is necessary for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Special category data which is processed for public health reasons or by a health professional for the purposes of preventative or occupational medicine.

4.4.5 You have one month to respond to the request, either to confirm you have complied with the request or informing the data subject why the request cannot be complied with. Please also notify the Council's Data Protection Officer if you are intending to refuse a request for erasure.

4.5 Right to restrict processing

4.5.1 Data subjects have the right to limit what their information can be used for. This may apply when it is not appropriate to erase their data or while you are considering a complaint or dispute in relation to the data.

4.5.2 Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

4.5.3 Restricting processing may also mean that the individual does not want you to delete information that you otherwise may have erased as part of your normal retention schedule.

4.5.4 There are several different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system.
- making the data unavailable to users; or
- temporarily removing published data from a website.

4.5.6 Restriction should only be a temporary measure while you assess the accuracy of the data, or whether your legitimate grounds override those of the individual. Once a decision has been made you should remove the restriction and inform the data subject.

4.6 Right to data portability

4.6.1 Data portability allows individuals to obtain and reuse their personal data, held in electronic form, for their own purposes across different services. This right only applies to information an individual has provided to a controller.

4.6.2 This right only applies if the information is being processed using consent or contract as the lawful basis.

4.7 Right to object to processing

4.7.1 A data subject has the right to object to you processing their data. A request can be made in writing or verbally and needs to be responded to within one month.

4.7.2 If the objection is in relation to direct marketing, then the request must be complied with.

4.7.3 It should also be considered if it relates to processing under the lawful basis of **Public Task** or **Legitimate Interests.**

4.7.4 You can continue to process the information if:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

4.7.5 You should notify the data subject of your decision, including your reasoning, within a month. If you refuse to comply with their request, you should **notify the Data Protection Officer** in advance of your response. It is important that the data subject is notified of their right to make a complaint to the ICO and their ability to seek to enforce their rights through a judicial remedy.

4.8 Exemptions to rights

4.8.1 There are a few circumstances where the rights of data subjects can be overridden, such as where the following would occcur.

- providing the information would be likely to prejudice crime or taxation.
- processing is in relation to legal proceedings or court records.
- in connection with health and safety.

4.8.2 There are further exemptions to the **right to be informed** and **right of access**. For example:

- data processed for the purposes of management forecasting or management planning in relation to a business.
- personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject which would be prejudicial to disclose.
- personal data consisting of a reference given (or to be given) in confidence.

4.8.3 There are further exemptions that only apply to the **right of access** such as:

- Where a relevant professional has confirmed that disclosing data concerning the data subject's health or social care records is likely to result in serious harm to themselves or others. Please note, where we hold information relating to the data subject's health or social care, which was provided by a relevant professional, it should not be disclosed to the data subject without the approval of that professional, unless we have evidence that the data subject is already aware of the information.
- Disclosing information to the data subject would involve disclosing personal data of a third party without their consent and it is not reasonable to do so.
- If the third party is a health professional, social worker, or education worker then you do not need their consent to disclose their name in relation to information about the data subject.

4.9 Process for challenging decisions

4.9.1 If information is withheld or a request is refused, and the data subject complains a review will be undertaken by the Data Protection Officer to establish whether the decisions taken were in line with the law using the ICO guidance.

4.9.2 Irrespective of whether the review upholds or overturns the decisions made when managing the original request, the outcome should be communicated to the requestor in a 'Review outcome letter' within a month and include any information which is being released as a result of overturning a decision to exempt information.

4.9.3 The review outcome letter should be sent to the Head of Law and Governance (Senior Information Risk Officer) for quality checking prior to sending.

5. Processing Children's data

Processing data relating to children should be done with special care as it merits particular protection under GDPR.

5.1 Consent

5.1.1 Children only have the capacity to consent if they are 13 years old or over. Therefore, you may need to verify their age if relying on a child's consent.

5.1.2 Even if the child is over 13 years old you still need to ensure they understand what they are consenting to otherwise the consent will not be 'informed' and therefore not constitute genuine consent. As a result, any wording needs to be clear, easy to understand and directed to the target audience.

5.1.3 If the child is under 13 years old you can get the consent of their parent or legal guardian. Where appropriate you may need to request proof of this legal responsibility such as a copy of a birth certificate.

5.2 Other factors when choosing a lawful basis for processing.

5.2.1 If using a contract as your lawful basis to process a child's data then you must consider the child's competence to agree to the contract and to understand the implications of the processing.

5.2.2 If using legitimate interests as your lawful basis you need to actively consider any risk to the child and take steps to safeguard against those risks.

5.3 Marketing to children

5.3.1 As well as complying with the rules around marketing to adults' specific protection needs to be given when marketing to children so that you are not exploit any lack of understanding or vulnerability. For example, making your wording or explanations clear and straightforward.

5.3.2 If a child objects to the marketing you should stop immediately.

6. Information Sharing

6.1 Sharing between internal departments

6.1.1 It is important to be aware that just because the information is held by a Council department does not entail that the information can be disclosed internally or freely used for purposes which are not compatible with the reason the information was collected in the first place.

6.1.2 In order to share personal data you need to identify the objective that sharing is meant to achieve, ensure only the information that is required to meet this objective is requested or shared and only with those employees who need to know.

6.1.3 To use personal data held by a Council department for another purpose you need to either:

- Gain consent from the data subject
- Apply an exemption listed in the Data Protection Act 2018
- Establish that the new purpose is compatible with the purpose the information was collected.

6.1.4 To request information from another department please fill in an '**Internal data sharing request form'** evidencing consent received or the reasons why you require the data.

6.1.5 The final decision whether to share will rest with the Council department that holds the information taking into account the justification provided.

6.1.6 Where a legitimate reason for sharing specific information between internal departments on a regular basis has been established, it is not necessary to fill out the individual sharing request forms. Instead, a formal procedure should be put in place to ensure that appropriate processes are followed when sharing the data to guarantee security and accountability. This may include undertaking a Data Protection Impact Assessment (DPIA).

6.2 Sharing with third parties, including the Police

6.2.1 The advice provided for sharing internally is also relevant to information sharing with third parties.

6.2.2 One-off requests should be documented. The third party should provide in writing the relevant exemption or lawful basis they are relying on with details of the purpose of sharing and why the information is necessary for that purpose. You can use the **Disclosure Request Form** to document a one-off request to share.

6.2.3 If a need for regular sharing has been identified then an **information sharing agreement** should be drafted between the relevant data controllers to establish the purpose and scope of the data sharing, specifying the security arrangements and retention periods.

6.3 National data opt-out for NHS data

6.3.1 The National data opt-out allows anyone who uses publicly funded health and/or care services to stop health and care organisations from sharing their "confidential patient information" with other organisations if it is not related to managing or delivering their individual care. For example, if this information is used for research or planning purposes.

6.3.2 As a result any information that is obtained from Health or Social Care partners or collected from our own care services can only be shared for purposes not directly linked to providing care to that individual, if they have been given the opportunity to opt-out of the sharing.

6.3.3 Where you process confidential patient data as part of your service and you intend to share this data with another organisation for a purpose other than delivering care, you will need to ensure that you have given them a chance to opt-out i.e. via tick box in a form, and you keep a record of this. Furthermore, the right to opt-out should also be clearly stated on your departmental privacy notice which is provided to the service user when their data is first collected.

6.4 Consent to share

6.3.1 If you are going to rely on consent as your condition to share you must be sure that individuals know precisely what data sharing, they are consenting to and understand its implications for them.

6.3.2 Consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so.
- the individual would be likely to object should the data be shared without his or her consent; or
- the sharing is likely to have a significant impact on an individual or group of individuals.

6.3.3 However it is bad practice to ask a data subject to consent if you will share the information anyway using a different lawful basis or exemption should they refuse. If this is the case you should still inform them that the sharing will occur and your legal basis for doing so, as this gives them the opportunity to object to sharing which we can consider in line with their right to object. However, you do not need to inform them if you are using an exemption and informing the individual of this sharing would prejudice the purpose the information was being shared for.

6.4 Other lawful basis for sharing

6.4.1 If you are not using consent then you have to ensure the purpose of sharing is compatible with the original reason for collecting the data. You also need to identify another lawful basis set out at 3.2.2 and an additional basis if sharing special category data set out at 3.2.3.

6.4.2 To determine whether the purpose is compatible you need to consider the following:

- any link between the purposes for which the personal data have been collected and the purposes of the intended sharing.
- the context in which the personal data have been collected, in particular the relationship between data subjects and the controller.
- the nature of the personal data. For example, high risk data such as special category or criminal convictions will require a strong basis for sharing.
- the possible consequences of the intended sharing for data subjects.
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

6.4.3 Information also needs be transparent which means any sharing that occurs or is likely to occur should be clearly stated on the relevant Privacy Notices. If this is not the case, then you should inform them of the sharing unless an exemption applies.

6.4.4 To ensure the sharing is fair, it needs to be reasonable and be something that people would be likely to expect and would not reasonably object to if given the chance.

6.5 Exemptions that allow sharing

6.5.1 Schedule 2, Part 1 of the Data Protection Act 2018 list exemptions from the obligation to be transparent, fair and only process for a specific limited purpose the data was collected for.

6.5.2 These include the following:

- data processed for any of the following purposes to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).
  (a)the **prevention or detection of crime**,
  (b)the **apprehension or prosecution of offenders**, or
  (c)the **assessment or collection of a tax or duty** or an imposition of a similar nature,

- information required to be **disclosed by law** or in connection with **legal proceedings.**

6.5.3 Although these exemptions allow you to share for another purpose it is up to the Council department to establish whether the information provided in the request is justified and proportionate.

6.5.4 If you are requesting information using an exemption or have received a request which requires an exemption to be considered you can use the **Disclosure Request form**

7. Roles and responsibilities

7.1 The Information Management Team (IMT)

7.1.1 The **Data Protection Officer (DPO)** is responsible for the following;

- Advising staff of their data protection obligations
- Regularly reviewing the Data Protection Policy and updating it as necessary.
- Monitoring Data Protection Training across the Council
- Contact point for Data Subjects and ICO
- Maintaining the Record of Processing Activities (Article 30 documentation)
- Ensuring Departments comply with the requirement to provide Privacy Notices
- Reviewing any complaints in relation to SARs or rights of the data subjects.
- Reviewing Data Protection Impact Assessments

Contact details: Natalie Lacey, dpo@runnymede.gov.uk

7.1.2 The Information Governance Officer (IGO) is responsible for;

- Ensuring corporate Council policies involving information are regularly reviewed and updated by the relevant teams.
- Monitoring Freedom of Information requests, to ensure responses do not breaching data protection law
- Monitoring Subject Access Requests and providing advice to departments on handling these requests

Contact details: Anthony Falce, foi@runnymede.gov.uk

7.1.3 The Head of Law and Governance is the SIRO and monitors the responsibilities listed in 7.1.1 and 7.1.2, taking on any urgent responsibilities if the DPO or IGO are not available.

Contact details: Mario Leo, mario.leo@runnymede.gov.uk

7.2 Information Champions (IC)

7.2.1 Each Council department or team will nominate an 'Information Champion' (IC) who will have oversight of data protection compliance and information governance arrangements within their team.

7.2.2 The IC should be senior enough to affect change but also be able to liaise with the Information Management Team on a regular basis. It is therefore expected that the IC's will be team leaders or middle managers.

7.2.3 The IC will be the first point of contact for the IMT in relation to data protection issues.

7.2.4 The IMT will provide IC with in depth training on data protection to ensure they can provide their departments with guidance on day to day data protection issues.

7.3 Information Governance Group (IGG)

7.3.1 The IMT will meet with the ICs quarterly to discuss corporate and departmental data protection/ information governance issues, and identify opportunities to promote good practice within the Council.

7.3.2 The ICs will feedback to their respective departments on the issues discussed at IGG.

7.3.3 The IMT will use the knowledge gained from the IGG to improve data protection and information governance policies and procedures and provide specific training for teams deemed high risk.

7.4 Management

7.4.1 Managers need to ensure their staff have completed mandatory data protection e-learning modules on an annual basis.

7.4.2 If training has not been completed this should be raised at the employee's appraisal.

7.4.3 Managers must ensure that an employee has reviewed this policy prior to accessing or processing personal data.

7.4.4 Managers should be aware of any data protection risks within their processes and flag these to their IC and the DPO.

7.4.5 Managers should address any data protection issues raised by staff. If they are unsure they should seek the advice of the IC, IGO or DPO.

7.5 Employees

7.5.1 All employees are responsible for undertaking the e-learning data protection training on induction and annually thereafter.

7.5.2 All employees must observe all forms of guidance, code of practice and procedures about the collection and use of personal information, including this policy.

7.5.3 If the employee is unsure of how to comply with this policy they should seek advice from their manager.

7.5.4 If an employee is undertaking a project they should consult the Data Protection Impact Assessment (DPIA) Procedure to confirm whether a DPIA is required.

7.6 Training

7.6.1 Training is an important part of ensuring staff are aware and fully understand council policies on protecting personal data.

7.6.2 As stated above it is both the employee and their manager's responsibility to ensure relevant data protection and data security training is undertaken at the appropriate times.

7.6.3 Information on the appropriate training can be found on our Data Protection/ Data Security & Information Governance Training Needs Analysis.

For all information contained within this document contact:

Runnymede Borough Council
The Civic Centre
Station Road
Addlestone
Surrey KT15 2AH

Tel 01932 838383

email: dpo@runnymede.gov.uk

www.runnymede.gov.uk

Further copies of this publication, or copies in large print other formats or languages can be obtained via the above contact details.

Search: Runnymede Borough Council