Renfrewshire Council

To: Finance & Resources & Customer Services Policy Board

On: 8 September 2022

Report by: Director of Finance and Resources

Heading: Data Protection Policy

1. **Summary**

1.1 The Data Protection Act 1998 ("DPA") regulated the processing of personal data and imposed obligations on the Council, as a data controller from 1 March 2000 until 25 May 2018. In response to this, the Council first introduced a Data Protection Policy in June 2001, outlining roles and responsibilities for data protection compliance. The policy is subject to review every two years. The most recent revisals were approved by Board in August 2020 to reflect the changes to data protection law made by the GDPR and the Data Protection Act 2018.

1.2 The Policy is now due for routine review. The proposed revisals are minor and mainly consist of explicit reference to "UK GDPR", which came into effect on 1 January 2021 and sets out the key principles, rights and obligations for most processing of personal data in the UK. It is based on the EU GDPR, which applied before that date in the UK, with some changes to make it work more effectively in a UK context. Although the Data Protection Act 2018 sets out the framework for data protection law in the UK, this sits alongside and supplements UK GDPR, for example, by providing some exemptions and setting out the Information Commissioner's functions.

1.3 The Data Protection and Digital Information Bill was recently introduced into Parliament. It is anticipated that this will be heavily debated and amended as it progresses through Parliament. For the time being, the UK GDPR and the DPA 2018 form the UK law on data protection. The Policy will be updated as and when the Bill becomes law.

2. Recommendations

2.1 It is recommended that the Council approve the revised Data Protection Policy, which forms the Appendix to this report, and agree that this continues to be reviewed on a two yearly basis.

---

3. Background

3.1 The Council is committed to data protection compliance and first approved a Data Protection Policy in June 2001. The purpose of a Data Protection Policy is to outline roles and responsibilities for data protection compliance. The Director of Finance and Resources is the Senior Information Risk Owner ("SIRO") for the Council. GDPR, as of 2018, required the Council to have a statutory officer, known as the Data Protection Officer. This role is discharged by the Managing Solicitor (DPO). Finance and Resources therefore take the overall lead in Data Protection and wider Information Governance matters. However, each Service and its senior management are obliged to retain a responsibility for data protection compliance. Given this devolved responsibility, each Service has a nominated data protection representative and depute. Service data protection representatives are members of the Council's Data Protection Working Group, which meets quarterly. The role of the Service data protection representative is to ensure data protection compliance within their Service, albeit advice can be obtained from the Data Protection Officer and the Information Governance team, at any time.

3.2 The policy continues to devolve responsibility to Services for departmental compliance, whilst also reflecting the statutory role of the Managing Solicitor (DPO) and the role of SIRO.

3.3 The Policy has been updated to include explicit reference to UK GDPR.

Implications of the Report

1. **Financial** – None.

2. **HR & Organisational Development** – HR & OD assist with training in and awareness of GDPR, by facilitating the launch of annual GDPR training.

3. **Community Planning –** N/A.

4. **Legal** – this Policy ensures ongoing compliance with data protection obligations.

5. **Property/Assets** – None.

6. **Information Technology** – ICT are essential to data protection compliance, given their cyber security and information management function and their lead role in relation to the Council's Information Asset Register.

7. **Equality & Human Rights** –

   (a) The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report. This policy seeks to ensure compliance with individuals' information rights. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.

8. **Health & Safety** – None.

9. **Procurement** – None.

10. **Risk** – this Policy supports the management of information risk, such as a potential data protection breach. Compliance is addressed on the Council's corporate risk register to ensure that the Council is fully compliant.

11. **Privacy Impact** – the Council has conducted Privacy Impact Assessments (PIAs) since 2013, as good practice in relation to projects or initiatives which involve processing personal information in new ways and have a potential privacy impact. Since May 2018, the Council has been conducting mandatory Data Protection Impact Assessments (DPIAs) as required to ensure compliance with data protection legislation and this Policy.

12. **Cosla Policy Position** – None.

13. **Climate Risk** – None.

List of Background Papers

N/A

Author: *Allison Black, Managing Solicitor (DPO)*
0141 618 7175
Alison.Black@renfrewshire.gov.uk

Renfrewshire Council

Data Protection Policy

Document History

Version	Date	Author	Reason for Issue/Change
1	June 2001	Craig Geddes, Archivist	
2	June 2012	Allison Black, Assistant Managing Solicitor	New governance arrangements
3	August 2014	Heather Semple Solicitor (Information Governance)	2-yearly update
4	August 2016	Heather Syme, Senior Solicitor (Information Governance)	2-yearly update
5	March 2018	Allison Black, Managing Solicitor (DPO)	Early update due to legislative change
6	August 2020	Allison Black, Managing Solicitor (DPO)	2 –yearly update
7	September 2020	Allison Black, Managing Solicitor (DPO)	2 – yearly

Document Review and Approval

Name	Action	Date	Communication
Andrew Connor, Records Manager	Consulted	March 2018	Email

Data Protection Working Group	Consulted	March 2018	Email
Data Protection Working Group	Consulted	February 2020	Email
ICT Enterprise Architecture Team	Consulted	February 2020	Email
Karen Locke, Risk Manager	Consulted	February 2020	Email

Related Documents

Ref	Document Name/ Version	Document Location
1	Guidance on Responsible Use of Personal Data and Confidential Information	
2	Records Management Policy	
3	Freedom of Information Policy	
4	Data Protection Guidelines	
5	Subject Access Request Guidelines	
6	Information Security Policy	
7	ICT Acceptable Use Policy	
8	Information Handling Policy	

Title	Data Protection Policy

Author	Allison Black
Issue Date	September 2022
Subject	Data Protection
Description	Renfrewshire Council's policy on data protection and issues surrounding data protection to ensure compliance with GDPR and the DPA 2018
Version	8.0
Source	Version 2 of the Data Protection Policy by Allison Black in August 2012
Updating Frequency	Two Yearly unless required earlier due to legislative change
Right	Not Protectively Marked.
Category	Data Protection

1. Introduction

1.1 The Council needs to collect and use information about people to discharge its functions. This Personal Data must be handled properly and lawfully and the Council is committed to data protection compliance and signed the Information Commissioner's 'Information Promise' as long ago as 2012.

1.2 Although data protection legislation is complex, its ethos is simple. It does what its title suggests and protects people's Personal Data by regulating the way in which organisations, such as the Council, handle this. In other words, it is legislation to regulate the processing of Personal Data.

1.3 The Data Protection Act ("DPA") 1998 imposed obligations on the Council, as a data controller, since 1 March 2000. However, as of 25 May 2018, the EU General Data Protection Regulation ("GDPR") and the DPA 2018 came into force. This was the biggest change to data protection law in twenty years.

1.4 GDPR and the DPA 2018 introduced a number of key changes, which were reflected in the updates to this Policy in 2018 and its review in 2020. On 1 January 2021 "UK GDPR" came into force. This now sets out the key principles, rights and obligations for most processing of personal data in the UK. It is based on the EU GDPR, which applied before that date in the UK, but with some changes to make it work more effectively in a UK context. Although the Data Protection Act 2018 continues to set out the framework for data protection law in the UK, this sits alongside and supplements UK GDPR, for example, by providing some exemptions and setting out the Information Commissioner's functions.

1.5 The Data Protection Principles

There are six Principles, which, cover rules for the maintenance, collection and security of personal data. The Council is committed to complying with the Data Protection Principles.

As such, the Council undertakes that Personal Data will:

1. Be processed fairly, 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.

Under UK GDPR, the Council needs to be able to demonstrate compliance with the principles. This is referred to as “accountability”.

1.6 The Council, in recognition of its data protection obligations, first approved a Data Protection Policy in June, 2001. Since then, a range of policies, procedures and guidelines promoting compliance and best practice, have been developed.

In addition to the Data Protection Policy, key Council documents include:

- Guidance on Responsible Use of Personal Data and Confidential Information,
- Information Handling Policy
- Records Management Policy,
- Freedom of Information Policy,
- Data Protection Guidelines,
- Subject Access Request Guidelines,
- Information Security Policy; and
- ICT Acceptable Use Policy.

This list is not exhaustive and all relevant data protection and wider information governance guidance can be obtained from the information governance section on the Council’s intranet.

2. Scope

This policy applies to all Services, employees and Elected Members of Renfrewshire Council and its Joint Committees and covers all Personal Data and Special Category and criminal offence data (formerly "Sensitive Personal") Data which they process. It may, however, be read alongside other Council policies and guidelines on use of non-personal data and wider information governance issues. Specific provisions relating to Special Category Data forming part of this Policy are annexed at Appendix 1.

3. Data Protection Governance Arrangements

3.1 Corporate Responsibility

The Council has a corporate responsibility for data protection and is defined as a "Controller" under UK GDPR.

3.2 Corporate Management Team and SIRO

The Director of Finance and Resources is the Senior Information Risk Owner ("SIRO") for the Council. The SIRO is supported in this role by the Managing Solicitor (DPO). The Managing Solicitor (DPO) reports to the Director of Finance and Resources, as SIRO, on information governance issues, including data protection compliance, on at least a monthly basis, and more regularly, as necessary. The SIRO and DPO report jointly to the CMT at least six monthly.

3.3 Statutory DPO

GDPR obliges the Council to have a statutory Data Protection Officer (DPO) on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The key tasks of the DPO are prescribed and are to:-

- Inform and advise the Council on GDPR compliance;
- Monitor compliance;
- Advise on Data Protection Impact Assessments;
- Train staff and

- Conduct internal audits
- Be the first point of contact for the regulator and
- Have due regard to the risk associated with the Council's processing operations.

3.4 SMTs

3.4.1 Each Service and its senior management will retain a departmental responsibility for ensuring data protection compliance.

3.4.2 All Services are required to nominate a departmental data protection representative of appropriate seniority and a depute.

3.5. Employees

3.5.1 All employees and Elected Members are individually responsible for ensuring that the processing of Personal Data is in accordance with UK GDPR and the DPA 2018 and should familiarise themselves and comply with Council data protection guidance. Advice can be obtained at any time from Information Governance Team.

3.5.2 The SIRO has overall responsibility for information governance. However, the day to day responsibility for driving the Council's information governance agenda is delegated to the Managing Solicitor (DPO).

3.5.3 The main role of the Service data protection representative will be to ensure compliance within his/her Service, by dealing with Service specific subject access requests, passing on advice and training and maintaining the accuracy of the Service's entries into the Council's Information Asset Register, detailed in paragraph 4.1. The Information Governance team will maintain an up to date list of Service data protection representatives.

3.5.4 The Records Manager will have a co-ordinating role in relation to subject access requests and will process any cross departmental subject access requests and any Finance and Resources requests. Although requests relating to only one Service are the responsibility of that Service, subject to any

guidance from the Records Manager and the Information Governance Solicitors, the Records Manager has oversight of all subject access requests.

3.5.5 The Information Governance Team and the DPO offer ad hoc advice on data protection issues.

3.5.6 The Senior Solicitors (Information Governance) have a key role in ensuring compliance with the sixth principle relating to data security by providing advice and guidance to Services on organisational information security, maintaining the Council's Information Security log and leading on information security incident management.

3.5.7. Cyber security and technical information security issues, including compliance with industry standards, are dealt with by the Council's Cyber Security Architect and Cyber Security officer, within the Enterprise Architecture Team in ICT Services. Responsibility for information management, which promotes efficiency when the Council processes information and extends beyond the processing of Personal Data, also lies with the Enterprise Architecture Team within ICT Services, who promote good information management by the provision of advice and guidance to Services.

3.6 Governance Groups and Working Groups

3.6.1 Each Service data protection representative is a member of the Data Protection Working Group ("DPWG"), which meets quarterly and is chaired by the Records Manager. The members of the DPWG each have the responsibility for dealing with data protection issues within their department and disseminating training and good data protection practice throughout their department. The remit of the DPWG is for each of these officers to discuss compliance within their Service, pass on advice and training, and process subject access requests which relate to records from their Services.

3.6.2 The DPWG operates as a sub group of the Information Management Governance Group ("IMGG"), which is jointly chaired by the Enterprise Architect and Managing Solicitor (DPO). The Records Manager and Senior Solicitor

(Information Governance) are also members of the IMGG. The IMGG consists of key officers with information management and information governance expertise. Although the remit of IMGG extends to wider information management and information governance issues, the Managing Solicitor (DPO), as co-chair, on behalf of the SIRO, will have the opportunity to manage and direct the agenda of IMGG to promote and progress the Council's information governance agenda. The Information Governance Team shall provide regular updates to the IMGG on the work of the DPWG.

3.6.3 The Information Security Group ("ISG"), which is chaired by the Chief Auditor and attended by the Managing Solicitor (DPO) and Senior Solicitors (Information Governance), also operates as a sub-group of the IMGG. The remit of the ISG is to support IMGG to ensure that information security is appropriate, proportionate, measured and embedded into business as usual. Membership of the ISG includes appropriate representation from ICT and Internal Audit.

4. Documentation of Processing Activities

4.1 Controllers are obliged to document their processing activities under GDPR (Article 30). There are some similarities between this obligation and the information previously provided to the ICO for notification under the old DPA 1998. The Council's Information Asset Register contains the Council's documentation of processing activities. This is known as an "Article 30 Register".

4.2 The Enterprise Architecture Team within ICT Services maintain the Council's Information Asset Register (IAR). This contains details of the Council's information assets, how those were obtained, how they are being used and who they are shared with. Each Service has an Information Asset Owner ("IAO"), who is the senior officer who oversees that Service's IAR entries. The IAO is assisted by an Information Asset Administrator ("IAA"). It is the responsibility of the nominated IAA to update the IAR and ensure that the entry for his/her Service is accurate at all times.

5. Data Subject Rights

5.1 Data subjects have several significant rights, 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

5.2 Further information on those rights is available in the Council's Data Protection Guidelines, available on the intranet and advice can be obtained at any time from the Information Governance Team. The right most frequently used by Council service users is the right of access, i.e. the right of an individual to access his/her own Personal Data. The Council has one calendar month to comply with subject access requests and must now do so free of charge. Further information on compliance with all data subject rights, particularly subject access rights, can be obtained from the Council's Subject Access Request guidelines, available on the Council's intranet, or from the Records Manager.

5.3 The Information Governance Team has responsibility for maintaining the Council's subject access request guidelines.

6. Training and Guidance

6.1 The Information Governance Team will continue to update detailed guidelines on the practicalities of dealing with UK GDPR and the DPA 2018 and oversee the implementation of the Council's Information Governance/ Data Protection Learning and Development Strategy. The purpose of this strategy is to ensure

that the learning and development needs of individual groups in relation to data protection and wider information governance are adequately addressed. The strategy identifies the training needs of Elected Members, Directors and Heads of Service, 3rd and 4th tier managers, employees who have specific requirements and those who require only a general awareness.

The existing guidelines, available from the Information Governance Team, or on the information governance section of the Council's intranet, familiarise officers with data protection compliance and the importance of information security and take account of guidance issued by the Information Commissioner, who enforces data protection.

7. Data Retention

7.1 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 Service 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.

7.2 The Records Manager, as outlined in the Council's Records Management Policy, provides advice on records management and retention issues.

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

8. Information Security

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

8.2 All employees and Elected Members have responsibility for keeping the Personal Data to which they have access, in the course of their work, safe and secure.

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

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

8.5 Employees and Elected Members who become aware of a potential breach of information security, such as a loss of data, must immediately report this to the Senior Solicitors (Information Governance), in line with the Information Security Incident Reporting Procedures.

8.6 Further information and advice on information security can be obtained from the Information Governance Team at any time and from the Council's Information Handling Policy and regular 'Think Twice' and SIRO bulletins.

9. Data Processors

If someone, other than an employee of the Council, is processing Personal Data on the Council's behalf, for example, a contractor or a consultant, the Council, as Controller, is obliged to have a written agreement with the Processor. The purpose of this is to ensure that the Processor will keep that information as secure as the Council would. Further information on Data Processor Agreements can be obtained from the Information Governance Team.

10. 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 and inter-departmental information sharing. There are many situations where information can, and indeed, must be shared, for example, to protect individuals. Detailed guidance on information sharing is available in the Council's Data Sharing Code

and advice can be obtained, at any time, from the Information Governance Solicitors. 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?

11. Data Protection Impact Assessments

11.1 The Council have conducted Privacy Impact Assessments (PIAs) under the old DPA for some time, as a matter of good practice. PIAs were carried out for any new initiatives or changes of business practice involving Personal Data.

11.2 The Corporate Management Team (CMT) first instructed in February 2013, that where policies and decisions have implications for the use of Personal Data held by the Council then all Services must conduct a PIA as an integral part of any project planning process rather than an add-on. Its purpose is to:

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

11.3 GDPR replaced voluntary PIAs with mandatory Data Protection Impact Assessments (DPIAs). Like PIAs, this is a process which enables the Council 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.

11.2 Advice on and assistance with carrying out DPIAs can be obtained from the Senior Solicitors (Information Governance).

12. Closed Circuit Television (CCTV)

12.1 Fair and Lawful Processing

The Council is a Controller of Closed Circuit Television (CCTV) and processes images lawfully, in accordance with the data protection principles and fairly by ensuring that data subjects have readily available to them the following information:

- the identity of the data controller;
- the purpose or purposes for which the data are processed; and
- any further information the data subjects should be given in the interests of fairness.

12.2 The ICO Code of Practice

The Council, in its use of CCTV, complies with the updated Code of Practice on the Use of CCTV and related guidance issued by the Information Commissioner. Operational procedures and training on CCTV provide more detailed information to staff on the deployment and maintenance of CCTV systems and the management of recorded images and monitoring stations.

12.3 Retention and Storage

Storage of images varies from system to system. Regardless of how they are stored, all images will be retained in accordance with established retention periods. The law does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage, but simply states that it should not be kept for longer than is necessary. After the retention period, the images are permanently deleted unless required for an ongoing issue which has been identified (e.g. if a crime has been observed and recorded or if the images have been retained whilst a SAR is being processed). In such cases images will be retained for as long as necessary (e.g. until the conclusion of any criminal proceedings arising from the incident or the SAR is completed).

Until deleted, all images are held securely in terms of the Council's operational procedures and this Policy.

13. Relationship with Other Legislation

13.1 Human Rights Act 1998

Public authorities, such as the Council, 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, the Council 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 data protection and the Freedom of Information (Scotland) Act 2002 ("FOISA") is complex. FOISA obliges the Council 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 from the Freedom of Information Guidance Manual, available from the Council's intranet, or the Records Manager and legal advice can be obtained at any time from the Information Governance Solicitors.

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 DPA to knowingly or recklessly obtain, access, disclose or procure Personal Data without the consent of the Data Controller. The Council 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

1. Introduction

UK GDPR and the DPA 2018 recognise that organisations are likely to collect information deemed Special Category Data and/ or Criminal Conviction and Offences data.

2. Definitions

UK GDPR Special Category data covers information about:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade Union membership.
- Physical or mental health or condition.
- Sex life and sexual orientation.
- Genetic data and biometric data.

Criminal and Offences Data or Conviction Data covers criminal allegations, proceedings or convictions and security measures. These are likely to centre on: specific employment requirements; fraud investigations; safeguarding issues; the vital interests of the data subject or other individuals.

3. Legal Basis

Under UK GDPR and the DPA 2018 the Council has a lawful basis for processing Special Category and Criminal offence data. The Council is obliged to collect and process this data and there is a substantial public interest in processing this information.

4. Procedures for Securing Compliance

The Council is obliged to have a policy for the processing of Special Category Data. Below are details of how the Council will comply with the Data Protection Principles in relation to the processing of Special Category and Criminal Offence personal data.

4.1. Principle 1 – Fair, Lawful and Transparent

Special Category and Conviction Data is processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Council will:

- Only process Special Category and Conviction Data where a lawful basis can be applied, and where processing is otherwise lawful.
- Process Special Category and Conviction Data fairly; and will ensure that data subjects are not misled about the purposes of any processing.
- Ensure transparency in its processing of Special Category and Conviction Data to enable individuals to understand and obtain their privacy information.

4.2. Principle 2 - Fit for Purpose

Special Category and Conviction Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The Council will:

- Collect Special Category and Conviction Data only for specified, explicit and legitimate purposes, and will inform data subjects what those purposes are in a privacy notice.
- Not use Special Category and Conviction Data for purposes that are incompatible with the purposes for which it was collected (if we do use Special Category and Conviction Data for a new purpose that is compatible, we will inform the data subject first).

4.3. Principle 3 – Data Minimisation (Adequate and Relevant)

Special Category and Conviction Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Council will:

- Only collect the minimum Special Category and Conviction Data needed for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

4.4. Principle 4 – Accuracy

Special Category and Conviction Data is accurate and, where necessary, kept up to date.

The Council will:

- Ensure that Special Category and Conviction Data is accurate, and kept up to date, taking care to do this where the use of this type of information has a significant impact on individuals.

4.5. Principle 5 - Data Retention

Special Category and Conviction Data will be 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.

The Council will:

- Only keep Special Category and Conviction Data in identifiable form. if is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once this data is no longer needed it will be deleted or rendered permanently anonymous.

4.6. Principle 6 - Security

Special Category and Conviction Data is processed in a manner that ensures appropriate security of the data including: protection against unauthorised or unlawful processing; against accidental loss, destruction or damage; and by using appropriate technical or organisational measures.

The Council will:

- Ensure that there are appropriate organisational and technical measures in place to protect Special Category and Conviction Data. Organisational protections include a robust information governance framework consisting of policies, procedures, guidance, training and awareness raising, including an ongoing 'Think Twice' campaign.

5. Accountability

The council is responsible for and must be able to demonstrate compliance with these 6 principles. The Managing Solicitor (DPO) discharges a monitoring role in relation to the Council's compliance with these principles.

The Council:

- Ensures that records are kept of all personal data processing activities, via its Information Asset Register ("Article 30 Register") and that these are provided to the Information Commissioner on request.
- Undertakes Data Protection Impact Assessments (DPIAs) for any high risk personal data processing, and consult the Information Commissioner if appropriate.
- Has a Data Protection Officer who provides independent advice and monitoring of personal data handling, and directly reports to the CMT on this.
- Maintains and reviews internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

- Ensures Council policies regarding the retention and destruction of personal data are implemented.

The Council ensures that where special category or convictions personal data is processed that:

- There is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- Where special category or criminal convictions personal data is no longer required for the purpose for which it was collected it will be deleted or render it permanently anonymous.
- Data subjects receive privacy information about how their data will be handled, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

6. Further Information

Further information on data protection can be obtained from the Managing Solicitor (DPO), the Information Governance Team or the Information Governance page of the Council's intranet.