South Ribble Borough Council

Data Protection Policy

Document Control

Document Title	Data Protection Policy
Version Number	5
Author	Kevin Conway
Approval Date	
Review date	12 months

1. Introduction

The Council keeps personal data to enable it to provide a wide range of services and to maintain record of the services provided. The information includes current, past and prospective employees, suppliers, clients/customers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments.

When personal data is collected and used, people's lives can be adversely affected if something goes wrong. For example, if details are not entered correctly individuals can be unjustly refused credit, benefits, housing or even a job. If data is not kept securely, an individual's privacy can be affected.

It is vital that those who collect, maintain and use personal information no matter how it is processed (i.e. in both paper and electronic format) maintain the confidence of those who are asked to provide it by complying with the requirements of Data Protection legislation.

2. Policy Statement

South Ribble Borough Council is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

3. Purpose & Scope of the Policy

This policy applies to:

- all part-time and full-time employees including those working from home or other remote/off site locations (including Shared Services staff)
- elected Members
- all other workers (including casual / agency workers, secondees and contractors) using the Council's equipment and computer network
- any other person permitted to use South Ribble Borough Council's computer resources

4. Responsibilities

- The **Chief Executive** has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation;
- The **Deputy Chief Executive** as **Senior Information Risk Owner** (SIRO) has responsibility**,** at executive level, for oversight of data protection and other aspects of information governance.
- The **Senior Team Leader Customer Services and Data Protection** as **Data Protection Officer** (DPO) has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate.

- **Directors and Assistant Directors** are responsible for ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and with Data Protection legislation; for assisting the DPO in their duties through providing all appropriate information and support; for ensuring that their staff are aware of their data protection responsibilities; and consulting the DPO on new developments or issues affecting the use of personal data in the organisation; for ensuring Data Protection Impact Assessments are conducted as appropriate on data processing activities in their business area, drawing on advice from the DPO
- **All colleagues** are responsible for understanding and complying with relevant policies and procedures for handling personal data appropriate to their role, and for immediately reporting any event or breach affecting personal data held by the organisation.

The Council will adopt and implement the policy set out in this document, thereby ensuring its compliance with Data Protection Legislation.

5. Data Protection principles

The General Data Protection Regulation (GDPR) is based on six data protection principles that apply to the processing of all personal data including storing, retrieving, using and the disclosure of information.

The principles state that personal data shall be–

- processed lawfully, fairly and in a transparent manner in relation to individuals.

- 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;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- 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;

- 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; and

- 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.

South Ribble Borough Council regards the lawful and correct treatment of personal information as critical to successful service delivery, and to maintaining the confidence of those with whom we work.

We must ensure that at all times the Council treats personal information lawfully and correctly.

The Council fully endorses the six principles of data protection as enumerated in the GDPR.

6. Individuals Rights

South Ribble Council will ensure that the rights of people about whom information is held can be fully exercised under the General Data Protection Regulation

These rights include:

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure (but see below)
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing

The right to erasure

The right to erasure is not absolute and only applies in certain circumstances.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- 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; or
- for the establishment, exercise or defence of legal claims.

Please note that in most cases South Ribble Borough Council will be processing data for the performance of a “public task”, for example, collecting Council Tax and will not be able to erase details.

The Council must act upon any request without undue delay and at least within one month of receipt.

7. Governance of Data Protection

We will maintain oversight and transparency in the management of personal data. We will meet our accountability duties through the maintenance of the following record-keeping systems:

- Up-to-date **privacy notice information** for colleagues, customers and service users;
- A **Record of Processing Activity (ROPA)** describing the content, purpose, controls and accountability for each data system or set of records holding personal data within the organisation
- A **log of information security incidents** impacting on personal data held by the organisation.
- Our Records of Processing Activities, under Article 30 of GDPR, will include all the information required to comply with paragraph 41 of Schedule 1 of DPA 2018 relating to special category data.

8. Data Protection by Design

We will apply Data Protection by Design principles to new systems and business processes through consulting the Data Protection Officer on the acquisition and development of new information systems and on proposals for significant new business processes and change.

Criteria for development and acquisition of ICT systems will include data protection compliance requirements for security and functionality.

As appropriate, the Data Protection Officer may advise the relevant head of Department to complete a Data Protection Impact Assessment in line with the organisation's template and guidance from the Information Commissioner's Office.

All contracts with organisations who are processing personal data on behalf of the organisation (data processors) will have GDPR-compliant contract clauses and be subject to appropriate levels of review and oversight. This will clearly set out expectations for how external contractors and suppliers must handle personal data relating to our colleagues, contacts and customers.

9. Data minimisation and accuracy

All colleagues must only record appropriate, accurate and relevant personal data in the course of their duties. This personal data must only be held on authorised forms and information systems – they must not be held on personal notes or devices.

Heads of Department must ensure that within their area of responsibility, ICT systems, forms and templates are kept under review to ensure that by design they only capture the minimum personal data necessary for the business activity.

10. Retention of personal data

Personal data must not be retained for longer than is necessary for the purpose for which it was gathered. Directors and Assistant Directors are responsible for ensuring that the Records Retention Schedule is applied to all records, data and documents holding personal data within their business area, by having regular or automated deletion or destruction of personal data in systems, paper files and on network folders. All documents and media containing personal data should be disposed of securely as confidential waste

11. Data Security incidents

Any security incidents which may impact on the confidentiality, integrity or availability of personal data held by us must be reported immediately to the Data Protection Officer by way of our Data Breach procedures (see separate document)
Such events could include:

- Loss of records, laptops or media containing personal data;
- Unauthorised access to information systems containing personal data;
- Access of personal data with no justifiable business need;
- Personal data being misdirected to an incorrect recipient;
- Loss of access to systems containing personal data.

All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

The Data Protection Officer will consider whether the incident meets the GDPR definition of a "personal data breach" which presents a risk to individuals. He/she will present a report to the SIRO including a recommendation on whether to report the matter to the Information Commissioner's Office (ICO).

If the SIRO decides that an incident constitutes a reportable data breach, the DPO will report the incident to the ICO and liaise as appropriate.

If a data breach presents a high risk to the data subjects, the DPO will ensure that they are also notified of the breach.

For further detail see the **Personal Data *Incident and Data Breach Reporting Procedure***.

12. Summary

South Ribble Borough Council will, through appropriate management, and strict application of criteria and controls, adhere to the following –

- Strive to collect and process only the data or information which is needed
- Use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted
- Strive to ensure information is accurate
- Not keep information for longer than is necessary
- Securely destroy data which is no longer needed
- Take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data)

- Ensure that information is not transferred abroad without suitable safeguards
- Ensure that there is general information made available to the public of their rights to access information

In addition, South Ribble Borough Council will ensure that:

- There is someone with specific responsibility for Data Protection in the organisation (the Data Protection Officer or DPO).
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Methods of handling personal information are clearly described.
- A regular review and audit is made of the way personal information is managed.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.