RYEDALE DISTRICT COUNCIL

ANNEX 3

Ryedale District Council

Information Governance Strategy and Policies

Responsible Officer: Data Protection Officer

Approval: Full Council

Audience: All Council Officers and Members

Date of Policy Enforcement: 25th May 2018

Date of Last Policy Review: -

Date of Next Policy Review: 25th January 2019

Version: 1.3

Contact Details of Data Protection Officer

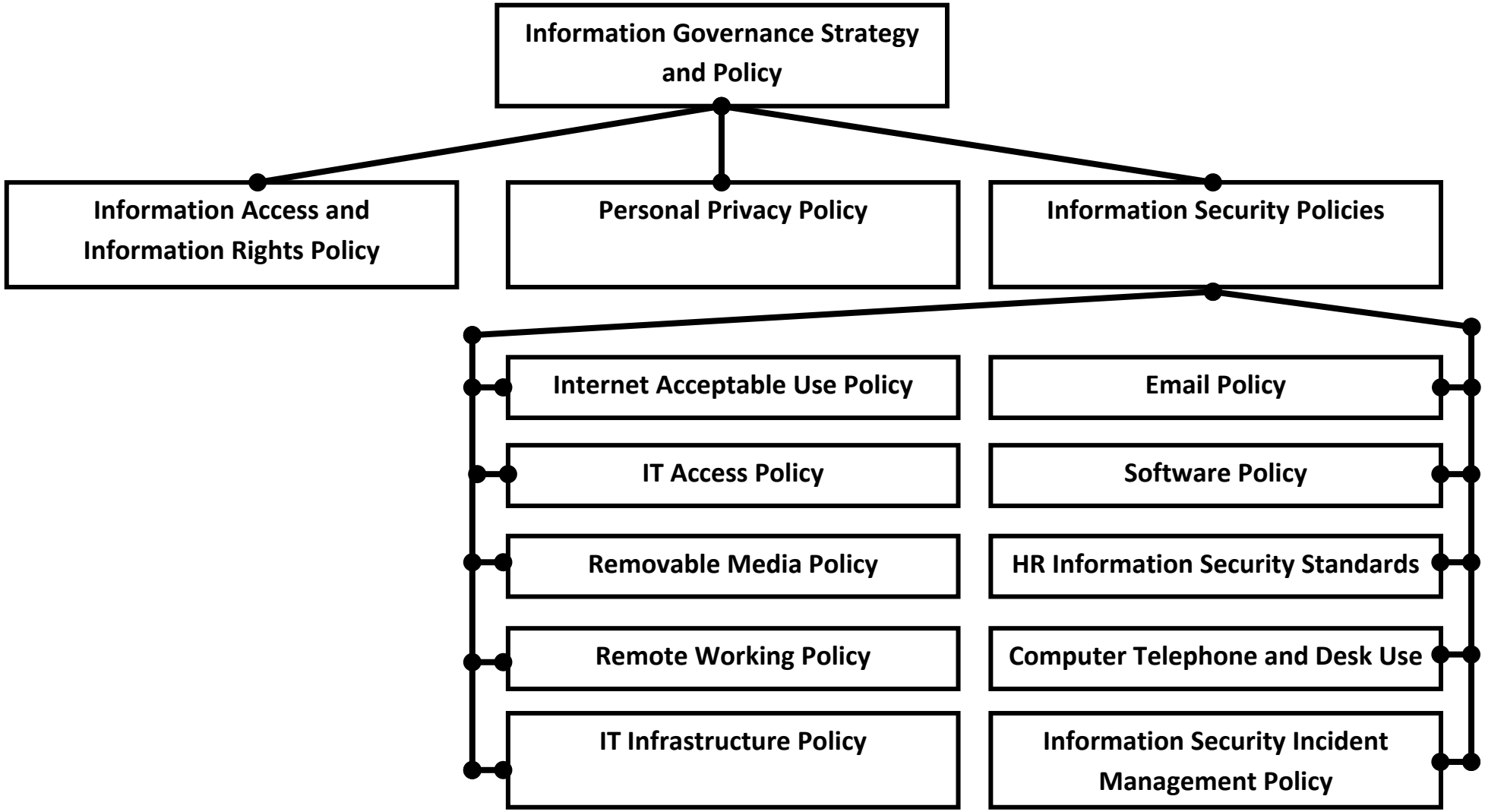
Name: *Information Governance Office, Veritau Ltd.*

Email: *DPA@ryedale.gov.uk*

Phone Number: *01609 53 2526*

Document Contents

RDC Information Governances Policy Structure Chart



Information Governance Strategy and Policy

1.0 Introduction

From May 2018 the UK's existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Ryedale District Council's (RDC) preparation for this new legislation, an Information Governance Strategy and Policy has been produced along with two new information governance policies:

- Information Access and Information Rights Policy
- Personal Privacy Policy

The Council has also reviewed its 'Information Security Incident Reporting Policy'.

Queries about any aspect of the Council's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at: DPA@ryedale.gov.uk

2.0 Scope

The Information Governance Strategy and Policy and corresponding policies apply to all Council officers, any authorised agents working on behalf of the Council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

3.0 Strategic objectives

The strategy aims to develop a robust information governance framework with the following features:

- There is effective oversight of information management matters at the top level of the organisation;
- The information governance policy suite is effective and accessible to all employees;
- The roles and responsibilities of the SIRO and Veritau (the Council's information governance advisors) are well established and widely known;
- A register of information assets has been compiled and information asset owners identified to ensure assets can be effectively managed and risks identified;

- Systems and processes are in place to securely store, transmit and dispose of information (both electronic and manual records);
- ICT Services implement technical solutions and procedures to protect personal data and minimise any potential security risks, including unauthorised disclosure of information, and seek national accreditation where appropriate;
- A layered framework of mandatory information governance training ensures employees receive information governance training commensurate with their role;
- A data protection officer has been appointed to support and direct compliance with GDPR;
- Systems have been implemented to enable information security incidents to be reported and investigated;
- Information security incidents are used to identify patterns and areas for improvement;
- Regular compliance checks are undertaken by internal audit, with the results used to shape future improvements;
- Key information risks are recognised on a specific information governance risk register and incorporated into the corporate risk register;
- Data Protection impact assessments are used to identify and address privacy risks associated with 'high risk' information processing, such as profiling;
- Personal information is collected and used responsibly, securely and fairly;
- Privacy notices are transparent and concise;
- Data subject rights are at the centre of service provision and understood by all employees;
- The Council is signed up to the Multi-Agency Information Sharing Protocol and information sharing with delivery partners has been formalised through written agreements under the protocol and subject to appropriate monitoring;
- Data processing arrangements are documented in a contract, which includes data processing clauses, and such arrangements are subject to appropriate monitoring;
- Any use of cloud computing technology is compliant with legislation; and
- Consider the value of signing up to codes of conduct and certification mechanisms as these become available.

An action plan has been produced to sit alongside this strategy. The action plan is regarded as fluid and subject to change and development as the Council reacts to business change, emerging information governance risks and as national guidance on the GDPR and DPA emerges.

4.0 Information Risks

One of the objectives of the Council's information governance strategy is to ensure the confidentiality, integrity and availability of information held by the council by reducing the risk of:

- Unauthorised access to data,
- Incomplete or inaccurate data,
- The unnecessary use of data;

Information risk management is the process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

Risks can never be eliminated fully. A structured, systematic and focused approach to managing risk is therefore required. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some degree of risk taking is inevitable and necessary if the council is to achieve its objectives. By being 'risk aware', the council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

5.0 Roles and responsibilities

- *Senior Information Risk Owner (SIRO):*
  The SIRO is responsible for the Council's overall information governance strategy and will be responsible for appointing the Data Protection Officer, the Specific Point of Contact, and the Information Asset Owners. The SIRO is accountable for the Council's compliance with information governance legislation.

- *Data Protection Officer (DPO):*
  The DPO is a statutory position and:
  - Is the point of contact for the Information Commissioner's Office (ICO) and data subjects;
  - Will facilitate a periodic review of the corporate information asset register and information governance policies;
  - Assist with the reporting and investigation of information security breaches; and
  - Will provide advice on all aspects of data protection as required, in particular data protection impact assessments and information sharing agreements.

- *Specific Point of Contact (SPOC):*
  The SPOC is responsible for overseeing the Council's day to day information governance practices and in particular facilitate the process for reporting information security breaches to the ICO.

The Council's information governance work will continue to be supported by specialist external advice from Veritau Limited, who will act as DPO.

The Council will also appoint Information Asset Owners to assist the SIRO in implementing the information governance framework.

6.0 Corporate Information Governance Group (CIGG)

The Corporate Information Governance Group is a quarterly strategic group focused on setting high level strategic objectives, shaping the policy framework, determining the acceptable level of information risk and monitoring the overall adequacy of the information governance arrangements.

CIGG will be comprised of the SIRO, who will chair the meeting, DPO and SPOC. The Council's Solicitor and IT Lead will also attend CIGG.

The current contact details for these officers are:

Senior Information Risk Owner (SIRO)	Peter Johnson Resources and Enabling Services Lead Peter.Johnson@ryedale.gov.uk
Specific Point of Contact (SPOC)	Simon Copley Principal Specialist for Democracy Simon.Copley@ryedale.gov.uk
Data Protection Officer (DPO)	Information Governance Team Veritau Limited DPA@ryedale.gov.uk
Council Solicitor	Anthony Winship Head of Legal Services Anthony.Winship@ryedale.gov.uk
IT Lead	Tim Sedman Principal ICT Enabling Officer Tim.Sedman@ryedale.gov.uk

Terms of reference for CIGG can be found at Appendix One.

7.0 Information Asset Management

In order for the Council to effectively manage the information that it holds and the risks associated with that information, it maintains an information asset management system.

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected, and exploited effectively. Information Assets have recognisable and manageable value, risk, content, and life cycles.

7.1 Information Asset Register

The Data Protection Officer (DPO) will assist the Council in developing and maintaining a corporate information asset register. The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format, location, and retention of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset
- Risk rating;

The register will be reviewed annually and Information Asset Owners will inform the DPO of any changes to their information assets as soon as possible.

7.2 Information Asset Owners

An Information Asset Owner (IAO) is a Council officer who is responsible for an information asset, understands the value of that information and the risks associated with it. The IAOs will be identified by the SIRO and DPO.

IAOs are responsible for ensuring the security and maintenance of their information assets. This includes ensuring other officers are using the information responsibly and safely. The role also includes determining the retention period for the asset and ensuring the information is securely destroyed in accordance with this period.

8.0 Training

The Council will provide basic training to all Council officers and elected members so that every Council employee is aware of the Council's responsibilities under Freedom of Information Act 2000, Environmental Information Regulations 2004, and Data Protection Act 2018. This includes all temporary staff and volunteers.

Training will be undertaken PRIOR to any individual being given access to Council systems or personal information. Advanced training will be given to officers who are expected to collate requested information and respond to requests for information.

Information governance training will be renewed annually for officers, and each time they are elected for elected members.

The Council will also ensure that third party contractors ensure their staff are adequately trained in information governance.

The SIRO is responsible for ensuring the training resources are effective and training requirements are adhered to.

9.0 Policy Publication and Review

The Information Governance Strategy and corresponding policies will be published on the Council's website and will also be available to Council officers and members via. the internal intranet.

The strategy and policies will be reviewed annually by the DPO. Any significant changes to the policy suite will need to be approved by the SIRO who has devolved responsibility from elected members to do so.

10.0 Key Messages

1. The Council's information governance strategy will seek to develop a robust information governance framework which is compliant with the requirements of the General Data Protection Regulation and Data Protection Act 2018

2. The Council will be 'risk aware', rather than 'risk averse' in respect of information risks

3. Key roles of Senior Information Governance Officer, Data Protection Officer, Specific Point of Contact and Information Asset Owners will support the delivery of Council's information strategy

4. The Council will maintain an Information Asset Register which will be used to manage information assets and risks.

5. Employees will be required to undertake mandatory information governance training commensurate with their role

Appendix One – CIGG Terms of Reference

1. Purpose

The Data Protection and Freedom of Information Acts place a specific responsibility on all organisations dealing with personal data to implement effective arrangements to ensure data is held securely, available to those who require that data and not disclosed to those not authorised to view it.

Within Ryedale District Council (RDC) the Resources and Enabling Services Lead has been designated as the Senior Information Risk Owner (SIRO) with specific responsibility for ensuring risks relating to Information Governance are managed effectively. The Corporate Information Governance Group (CIGG) exists to support the SIRO in the discharge of those responsibilities and promote a culture of responsible and effective information governance practice within the Council.

The Policy and Resources Committee of the Council also has the authority to review all corporate policies and procedures in relation to Information Governance, and to oversee the implementation of Information Governance policies and procedures throughout the Council.

2. Core Responsibilities

The role and responsibilities of the Group are as follows:

- Identify and develop an Information Governance strategy to enable RDC to comply with its legal obligations;
- Maintain an appropriate information governance policy framework which reflects current best practice;
- Manage corporate information risks, including determining the acceptable level of risk;
- Monitor the effectiveness of information governance policies, and associated documents, identify new legislation and guidance and update policies and procedures where necessary;
- Monitor compliance with corporate information governance policies and procedures, and implementing corrective action where necessary;
- Develop appropriate action plans to support the achievement of the Information Governance Strategy;
- Maintain procedures for dealing with information security incidents and ensuring improvements are implemented;
- Promote and implement training and learning designed to encourage improvement in relation to information governance practices;
- Discuss problematic information governance issues and identify/approve appropriate solutions
- Report annually to the Overview and Scrutiny Committee on information governance activity

3. Membership

The following officers will make up the membership of CIGG:

- Head of Resources and Enabling Services (SIRO/S.151 Officer)
- Principal Specialist Democracy
- Principal ICT Enabling Officer

- Head of Legal Services
- Data Protection Officer

4. Frequency of Meetings

The Group will meet quarterly with effect from April 2018. A quorum shall consist of a simple majority of members. If the Chair is unavailable then the meeting will be re-arranged. If unable to attend, members may (with the agreement of the Chair) nominate a deputy to attend in their place.

5. Agenda and Minutes

Agendas will be issued one week prior to meetings taking place. Meeting minutes will be taken at the meeting for record of decisions made.

Personal Privacy Policy

1.0 Introduction

From May 2018 the UK's existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Ryedale District Council's (RDC) preparation for this new legislation, an Information Governance Strategy and Policy has been produced along with two new information governance policies:

- Information Access and Information Rights Policy
- Personal Privacy Policy

The Council has also reviewed its 'Information Security Incident Reporting Policy'.

Queries about any aspect of the Council's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at: DPA@ryedale.gov.uk

2.0 Scope

This policy applies to all Council officers, any authorised agents working on behalf of the Council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

3.0 Data Quality

The Council is committed to the collection and use of high quality data which is 'right first time' and can be relied upon for decision making and performance review. The personal privacy policy is intended to help the Council improve its decision-making and performance management by having:

- Sufficient information to support decision making;
- Data that is accurate, reliable and subject to periodic verification;
- Data that is up to date and used in a timely way;
- Data that can be shared productively within and outside the Council;
- Systems that support the production of relevant and reliable data;
- Procedures to ensure that staff are aware of their responsibilities;

- Training to maintain and improve the quality of the Council's data;
- Skills and tools to analyse and interpret the information; and
- Skills and knowledge to present the information in an informative and meaningful way.

Data quality not only refers to numbers and statistics but also includes other information that the Council may process. Names, addresses and other types of information must be recorded accurately on council systems.

There are six key characteristics of good data quality as follows:

Accuracy	Data should be sufficiently accurate for its intended purposes, representing clearly and in sufficient detail the interaction provided at the point of activity. Data should be captured once only, although it may have multiple uses. Accuracy is most likely to be secured if data is captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable informed decision making at all levels. The need for accuracy must be balanced with the importance of the uses for the data, and the costs and effort of collection. For example, it may be appropriate to accept a lower degree of precision where timeliness is important. Where compromises have to be made on accuracy, the resulting limitations of the data should be clear to its users.
Validity	Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will ensure consistency between periods and with similar organisations. Where proxy data is used to compensate for an absence of actual data, organisations must consider how well this data is able to satisfy its intended purpose.
Reliability	Data should reflect stable and consistent data collection processes across collection points and over time, whether using manual or computer-based systems, or a combination. Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.
Timeliness	Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence the appropriate level of service or management decisions.
Relevance	Data captured should be relevant to the purposes for which it is used. This entails periodic review of requirements to reflect changing needs. It may be necessary to capture data at the point of activity which is relevant only for other purposes, rather than for the current intervention. Quality assurance and feedback processes are needed to ensure the quality of such data.
Completeness	Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

4.0 Privacy Notices

The Council will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. A corporate privacy notice will be displayed on the Council's webpage in an easily accessible area, and will be supplemented by service specific notices. The notice will also be available in hard copy for those who request it.

Where possible, data subjects will be provided with a privacy notice before their data is obtained by the Council. If this is not possible then it will be provided to the data subject as soon as possible after the Council has obtained their data.

Privacy notices should be cleared by the DPO prior to being published. A record of privacy notices shall be kept on the Council's Information Asset Register.

5.0 Information Sharing

In order to operate efficiently and provide the optimum service to data subjects it is sometimes necessary to share personal information with third party organisations. Routine and regular information sharing arrangements will be documented in an information sharing agreement (see below).

All information sharing agreements and any adhoc information sharing will be authorised by the information asset owner.

5.1 Multi-Agency Information Sharing Protocol

Ryedale District Council is a signatory to the North Yorkshire Overarching Multi-Agency Information Sharing Protocol (the Protocol). This means that when sharing information with another signatory Partner the Council should follow the procedures and best practice laid out in the Protocol & associated pro-formas.

The Council will use the Multi-Agency Information Sharing Protocol's 'Annex J' pro-forma when developing such agreements with non-signatory Partners.

When transmitting personal information the responsible officer will ensure that appropriate security safeguards are in place.

5.2 Documenting Information Sharing

All disclosures of information should be accurately recorded. Officers should take care to record when and how information is disclosed to third parties.

The Data Protection Officer is required to advise on all information sharing agreements and will keep a register of completed information sharing agreements.

6.0 Data Protection Impact Assessments (DPIA)

The Council will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The IAO is responsible for ensuring the completion of the DPIA. The DPO must advise on such assessments.

High risk data processing projects where it is not possible to mitigate the risks to an acceptable level may require authorisation from the Information Commissioner's Office. The DPO will advise where this is the case and will liaise with the ICO, following consultation with the SIRO. The DPO will keep a register of completed assessments and ensure that officers have access to a current assessment template.

7.0 Retention Periods

Retention periods will be determined by any legal requirement, any best practice or national guidance, and lastly the business need to retain the information.

In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

7.1 Destruction of Records

Retention periods for records are recorded in the Council's information asset register. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins.

ICT helpdesk will provide advice to officers on secure destruction of electronic media.

A record should be retained of all files destroyed which includes, where relevant:

- File reference number,
- Description of file,
- Date of disposal,
- Method of disposal,
- Officer who destroyed record,
- Authorising IAO;

In exceptional cases upon reaching the end of its retention period an IAO may consider it necessary to assign a new retention period for that individual record, for example Ombudsman involvement may necessitate records being kept for longer than usual.

8.0 Third Party Data Processors

All third party contractors who process data on behalf of the Council must be able to provide assurances that they have adequate data protection controls in place to ensure that data that they process is secure.

The Council's standard terms and conditions will include data processor clauses. A standard set of data processor clauses can be found in Appendix One of this Policy.

The SIRO may insist that any data processing, by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place.

If any data processing is going to take place outside of the UK then the Data Protection Officer must be consulted prior to any contracts being agreed.

9.0 Key Messages

1. The Council will ensure procedures are in place to ensure data is high quality so that it can be used for decision making and performance review.

2. The Council will publish Privacy Notices to communicate how its uses the personal data of its service users.

3. The Council will ensure information shared with other organisations is well documented and within the limits of the law.

4. The Council will carry our Data Protection Impact Assessments for all new projects that involve the processing of high risk personal data.

5. The Council will maintain a retention schedule and will ensure information is securely destroyed upon expiration.

6. The Council will include Data Protection processing clauses in all of its contracts and service level agreements.

Appendix One – Data Processing Clauses

To be developed by Veritau – Due for completion mid Feb

Access to Information and Information Rights Policy

1.0 Introduction

From May 2018 the UK's existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Ryedale District Council's (RDC) preparation for this new legislation, an Information Governance Strategy and Policy has been produced along with two new information governance policies:

- Information Access and Information Rights Policy
- Personal Privacy Policy

The Council's information security policies have also been updated.

Queries about any aspect of the Council's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at: DPA@ryedale.gov.uk

2.0 Scope

This policy applies to all Council officers, any authorised agents working on behalf of the Council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Freedom of Information (FOI) requests generally applies to all information held by the Council subject to certain exemptions. FOI does not apply to private correspondence of officers and elected members nor does it apply to party political documents or party political correspondence held by elected members.

Environmental Information Regulations (EIR) requests apply to all environmental information held by the Council subject to certain exemptions.

Data Protection Requests, known as Subject Access Requests (SAR), apply only to the personal information of the data subject – that is the person who the data is about. Only the data subject, someone legitimately acting on their behalf, a legally appointed advocate of the data subject, or a third party who has the explicit consent

of the data subject should be permitted to access this data. The right of access is subject to certain exemptions.

This policy also covers specific rights, prescribed by the Data Protection Act 2018 and the General Data Protection Regulation, that data subjects have in relation to information that the Council may hold about them.

All of these rights apply to all information held by, or on behalf of the Council, regardless of format. This could be reports, emails, memos or even photographs.

3.0 Responsibilities under Local Government (Access to Information) Acts and Transparency Codes

The Council is required, under variations of the Local Government Act, to publish and make information available to ensure decision making is transparent and accountable. The Council will therefore:

1. Provide information under the Citizen's Charter about public services, what those services cost, targets, performance, complaints, and redress;
2. Issue monthly forward plans;
3. Publish internal departmental guidelines when dealing with the public;
4. Give 3-days prior access to reports , agendas, and background papers for decisions;
5. Ensure that key decision making meetings are open to the public and produce a record of, with the reasons for, such decisions;

The Council is also obliged to comply with the Local Government Transparency Code (2015) which stipulates the Council must publish various information, such as Payments of over £500 and the salaries of senior officers, in order to be transparent in the way that it operates.

The Council will make its transparency information available to the public via. a dedicated webpage. It will be the responsibility of the relevant service manager to ensure that this information is published according to the legislative time periods. Appendix One contains a list of transparency information that is required to be published, the timescales for publishing, and the manager responsible for publication.

4.0 Requests for Information under Freedom of Information Act 2000 and Environmental Information Regulations 2004

Each corporate director is responsible for managing information within their business area. This includes responding to information requests. Usually, corporate directors will delegate any information request to a 'responsible officer' with appropriate seniority and authority within the service to which the request relates. This may be the relevant information asset owner (IAO) for the information requested. Corporate directors must ensure that responsible officers reply to the request within the statutory time limits.

The responsible officer is responsible for:

- Deciding whether the information requested is held;
- Locating, retrieving or extracting the information;

- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester.

4.1 Receiving A Request

Any officer, elected member, or third party contractor could receive a request for information. When such a request is received it should be passed immediately to the customer service centre for processing.

Each request received by the Council will be acknowledged with the applicant within 5 working days by the Customer Service Centre.

The customer service centre will log the request, provide a reference number and forward the request onto the responsible officer to respond.

EIR requests do not need to be submitted in writing and can be submitted orally. However the responsible officer should write this request down for the responsible officer to confirm in writing the details of the request with the applicant.

4.2 Timescales and Fees

The Customer Service Centre is responsible for compliance with FOI/EIR timescales.

The circumstances under which the Council may impose a charge are extremely limited. Any charges will be imposed in accordance with the Council's charging regime, which can be found at appendix 2.

4.3 Searching for Information

When locating information across council filing systems, databases, and archives (electronic and manual) officers should take care to search variations of file names. Officers should make a record of what search terms they used and what systems were searched.

4.4 Exemptions

There are a range of exemptions and exceptions, both in FOIA and EIR, which may be applied to intended disclosure. Often these exemptions are subject to the public interest test where the responsible officer must decide if it the public interest in withholding the information outweighs the public interest in disclosing the information. If the responsible officer is of the opinion that an exemption may apply, he or she should seek advice from their service manager or the Legal Services Manager before withholding the information.

4.5 Responding to Requests

If an information request relates to information which is held across a number of directorates with different responsible officers, each responsible officer is responsible for locating the information held by their respective directorate. They should provide their draft response to the Customer Service Centre who will coordinate and prepare a consolidated reply.

Applicants are able to request hard copies of the information or electronic copies of the information. The Council is not obliged to comply with a particular format unless it is reasonable to do so. All responses will be sent electronically where possible. Where copy documents are requested there is no requirement to send a copy of the document to the applicant. In some cases it may be easier to extract the information from the document or to provide a digest.

Officers should take care to ensure redactions are permanent and cannot be reversed.

When responding to any request which is potentially sensitive or controversial the responsible officer will consider where any additional senior management approval might be required prior to responding to the request.

4.6 Publication Scheme

The Council will adopt the Information Commissioner's model publication scheme.

Fees for printed publications or for information held on the Local Land Charges Register will be published in the publication scheme.

The publication scheme will be maintained by the Principle ICT Enabling Officer and reviewed on an annual basis.

Prospective FOI/EIR applicants will be advised to refer to the publication scheme prior to submitting a request for information.

4.7 Re-use of Public Sector Information Regulations 2015

The Reuse of Public Sector Information Regulations 2015 (RPSI) allow individuals or organisations to reuse information, originally created to fulfil public task, for other purposes. Importantly RPSI is about re-use of information only – access to information will still be dealt with under the usual access to information legislation.

The Council expects to be able to grant reuse to most information, but can impose certain restrictions on re-use. If this is the case it will apply Open-Government Licensing terms and conditions unless exceptional circumstances deem that it is not appropriate to do so.

5.0 Requests for Personal Information under Data Protection Act 2018 (Subject Access Requests)

The DPA gives data subjects the right to access their own information that the Council holds about them. This is known as a Subject Access Request (SAR).

5.1 Receiving a Request

Any officer, elected member, or contractor of the Council could receive a request from an applicant at any time.

The DPA 2018 does not require subject access requests to be made in writing. However, applicants will be encouraged to complete the 'Subject Access Request Form' where possible, to ensure that all necessary information is required.

Requests that are received orally will be written down by the receiving officer and confirmed with the applicant by the responsible officer to ensure the council understands the applicant's request.

All requests for personal information must be passed to the Legal Services Manager who will log on the Council's corporate register and assign a reference number. The Legal Services Manager will be responsible for responding to the request.

The Council must be satisfied as to the applicant's identity. If the responsible officer is not certain of the applicant's identity from existing Council records or involvement with the applicant, they may ask that that applicant produce:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- Or enough information for the council to be satisfied of the applicant's identity;

5.2 Timescales and Fees

No fee may be charged for processing a request.

A request only becomes valid once the Council is satisfied it has sufficient detail to respond to the request; it has 30 calendar days to respond.

The Council can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either complexity of the case or volume of the information. If the Council wishes to apply an extension they will inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads.

In very limited cases the Council may also refuse a request outright as 'manifestly unreasonable' if the Council would have to spend an unjustified amount of time and resources to comply.

5.3 Searching for Information

When locating information across council filing systems, databases, and archives (electronic and manual) officers should take care to search name variations, initials, and nicknames. Officers should make a record of what search terms they used and what systems were searched.

5.4 Exemptions and Third Party Information

There are a range of exemptions, in the Data Protection Act, which can be applied to some or all of the information being requested. A data subject's right to their own data is very strong and the Council will only apply exemptions when absolutely necessary.

Third Party data, that is data about a person other than the data subject, should also be withheld from the disclosure unless:

- The third party individual has given consent;
- They are incapable of giving consent; or
- There is a reasonable expectation of disclosure (i.e the third party is a Council officer or other professional working with the data subject);

5.5 Responding to Requests

Subject Access Requests must be answered within the timeframes stipulated above (5.2).

If an information request relates to information which is held across a number of directorates with different responsible officers, each responsible officer is responsible for locating the information held by their respective directorate. They should provide their draft response to the Legal Services Manager who will coordinate and prepare a consolidated reply.

The Council is obliged to send responses in the same format as the request was received – every effort will be made to comply with this requirement. If an applicant requests the information in a specific format the Council is not obliged to comply unless it is reasonable to do so. Where copy documents are requested there is no requirement to send a copy of the document to the applicant. In some cases it may be easier to extract the information from the document or to provide a digest. .

Officers should take care to ensure redactions are permanent and cannot be reversed.

6.0 Other Rights of the Data Subject

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR and Data Protection Act 2018:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to Legal Services Manager who will acknowledge the request, log the request on the central register and assigned a unique reference number. The Legal Services Manager will ensure the request is responded within 30 calendar days.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

7.0 Complaints

The Freedom of Information Act and The Environmental Information Regulations require a statutory internal review process. An applicant can ask the Council to review its handling of an FOI/EIR request, including:

- Any exemptions that have been applied;
- Any information they believe to be missing;
- That proper procedures have not been followed in responding to a request;

All responses to requests will include contact details to request an internal review.

Requests for internal review should be passed to the Specific Point of Contact (SPOC) who will review the case and respond to the applicant within 20 working days.

If an applicant is not satisfied with the outcome of an internal review they may request an independent review by the Information Commissioner. The SPOC will act as the point of contact for the Information Commissioner in respect of FOI/EIR complaints.

The Data Protection Act does not have a statutory internal review mechanism. However, it is considered best practice for organisations to have a complaints procedure.
Therefore, any complaints about subject access requests should be directed to the Data Protection Officer who will respond to the applicant within 20 working days.

8.0 Key Messages

1. The Council will routinely publish statutory datasets under open government legislation

2. The Council will operate a robust system to comply with requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 and requests for personal information under the Data Protection Act 2018

3. A corporate log of FOI/EIR requests will be maintained by the Customer Service Centre and a corporate log of requests exercising rights under the General Data Protection Regulation & Data Protection Act 2018 will be maintained by the Legal Services Manager

4. Internal reviews for FOI and EIR requests will be responded to by the Specific Point of Contact and internal reviews for Subject Access Requests will be responded to by the Data Protection Officer.

Appendix One – Transparency Information for Publication

Transparency Information	Publication Frequency	Responsible Officer
Payments of over £500	Monthly	Resources & Enabling Services Lead (s151)
Government Procurement Card transactions	Monthly	Resources & Enabling Services Lead (s151)
Relevant procurement information	Varied	Resources & Enabling Services Lead (s151)
Land and building Assets owned by the Council	Annual	Resources & Enabling Services Lead (s151)
Social Housing Asset Value	Annual	Resources & Enabling Services Lead (s151)
Grants to Voluntary, Community, and Social Enterprise organisations	Annual	Resources & Enabling Services Lead (s151)
Organisation Chart	Annual	Deputy Chief Executive
Trade union facility time	Annual	Deputy Chief Executive
Income and Expenditure from Parking Accounts	Annual	Frontline & Delivery Services Lead
The number of marked out parking spaces in the authority's boundaries	Annual	Frontline & Delivery Services Lead
Salaries of senior officers	Annual	Deputy Chief Executive
The Council's Constitution	Annual	Council Solicitor
Pay policy statements and pay multiple data	Annual	Deputy Chief Executive
Counter Fraud statistics	Annual	Resources & Enabling Services Lead (s151)
Waste Contracts	Upon Completion	Frontline & Delivery Services Lead

Appendix Two - Standard Costs To Be Used in the Calculation of Fees For Requests Under The Freedom Of Information Act 2000

Staff time	£25.00 per hour
Photocopying Costs	10p per copy
Printing Costs	10p per copy
Postage Costs	1st class at cost or original estimate, whichever is lesser
Other items such as relevant translation	At cost or original estimate, whichever is lesser

CHARGING REGIME

Fee is less than £5.00	No charge will be made
Cost of fee between £5.00 and £450.00	If the cost to service a request is estimated at between £5.00 and £450.00 (approximately 17 staff hours plus £25 disbursements) then a charge for non-staff costs as above will be made
Cost of fee is over £450.00 (*)	If the cost to service a request is estimated to cost in excess of £450.00 (more than 17 staff hours plus £25 disbursements) then the full cost, including staff time at the above rate, will need to be charged
Aggregation of Requests	If two or more requests are received within 60 consecutive working days, for the same or similar information either from the same person or different persons who appear to be acting as part of a campaign, then the charges will be aggregated. Once the cost exceeds £450.00 then the full costs, including staff time, will need to be charged
Mixed Requests	If a request is received in which the information is covered by more than one access to information regime then, for the purposes of calculating fees, it is necessary to separate out the constituent parts of the request to determine what fee may be charged. The above charging regime is applicable to the FOI element.

*** Where the fee is calculated at over £450.00**

Where the fee is calculated at over £450.00 Section 16(1) requires the Council to provide advice and assistance, "so far as it would be reasonable to expect the authority to do so, to persons who propose to make, or have made, requests for information"	Stage 1 – If the request is particularly wide-ranging, and therefore likely to be expensive to answer, the Council must discuss this with the applicant to see if the question could be refined to a more manageable level to bring it below the £450 limit.
	Stage 2 – If after providing advice and assistance, as required under Section 16, the request is still over the appropriate limit the Council can **either** turn the request down or answer the request and charge a fee.
	Or where the Council decides to provide the information and charge a fee, and does not have other powers to do so, the Council can charge on the basis of the costs outlined above, as well as the cost of informing the applicant whether the information is held and communicating the information to the applicant.

Information Security Incidents Reporting Policy

1.0 Introduction

From May 2018 the UK's existing Data Protection Act will be replaced by the EU's General Data Protection Regulation and the Data Protection Act 2018. As part of Ryedale District Council's (RDC) preparation for this new legislation, an Information Governance Strategy and Policy has been produced along with two new information governance policies:

- Information Access and Information Rights Policy
- Personal Privacy Policy

The Council has also reviewed its 'Information Security Incident Reporting Policy'.

Queries about any aspect of the Council's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at: DPA@ryedale.gov.uk

2.0 Scope

This policy applies to all Council officers, any authorised agents working on behalf of the Council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

3.0 Notification and Containment

Article 33 of the GDPR compels data controllers to report breaches of personal data, to the Information Commissioner's Officer, within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that the Council has a robust system in place to manage, contain, and report such incidents.

3.1 Immediate Actions (Within 24 Hours)

If a Council officer, member, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Specific Point of Contact (SPOC) within 24 hours. If the SPOC is not at work

at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the officer who located the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

3.2 Assigning Investigation (Within 48 Hours)

Once received, the SPOC will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

WHITE	Information security event No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
GREEN	Minimal Impact A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary.
AMBER	Moderate Impact The Council's security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.
RED	Serious Impact A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.

The SPOC will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The SPOC will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

3.3 Reporting to the ICO/Data Subjects (Within 72 Hours)

The SIRO, in conjunction with the service manager, SPOC, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The service manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

4.0 Investigating and Concluding Incidents

The SPOC will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the Council.

5.0 Key Messages

1. All officers, elected members and Council contractors must notify the Council's Specific Point of Contact, within 24 hours, when an Information Security Incident has occurred.

2. The Council's Specific Point of Contact will assign a severity rating to the incident and assign investigation. The most serious incidents will be assigned to the Council's Data Protection Officer (Veritau Ltd) for investigation.

3. The SIRO will be responsible for deciding if an Information Security Incident needs to be reported to the ICO or the Data Subject. The SIRO will take advice from the IAO, the SPOC and the DPO.

4. The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

Version Control

Version Number	Summary of Changes	Officer	Date
V 1.0	Draft Policy	Matt North (Information Governance Officer, Veritau)	09/01/2018
V 1.1	Draft – Comments from Senior Officer	Louise Jackson (Senior Information Governance Officer, Veritau)	15/01/2018
V 1.2	Draft – Modifications after first CIGG Meeting	Matt North (Information Governance Officer, Veritau)	17/01/2018
V 1.3	Final First Draft – Following comments from CIGG members	Matt North (Information Governance Officer, Veritau)	20/02/2018