Subject: **Records Management and Data Protection**

Report to: **Policy and Resources Committee**

Report by: **Corporate Services Manager/Interim Data Protection Officer (DPO)**

SUBJECT MATTER/RECOMMENDATIONS

1) The Policy and Resources Committee are asked to approve the Record Management Policy.

2) That it be noted that an updating report has been drafted by the Interim Data Protection Officer for the Members oversight of the Borough Council's compliance with the General Data Protection Regulation 2016/679 (EU) ('GDPR') and the Data Protection Act 2018 ('DPA2018').

1. INTRODUCTION/BACKGROUND

This report provides an update on Great Yarmouth Borough Council's compliance with GDPR and the DPA2018:

Issue	Synopsis
1. Records Management Policy	The new Records Management policy is for senior leadership review and approval.
2. Data Retention	It is advised that the Heads of Service coordinate a review and update of all the Council's data retention policies across their services areas, liaising with Emma Pheby (the new DPO).
3. Data Storage	A review of data storage across all service areas, led by the Heads of Service, liaising with the DPO, as required.
4. Data Deletion	Data deletion to be taken after a thorough review of data retention. This should be done in line with the Council's new Records Management Policy ensuring systematic and authorised deletion.
5. Data Breaches	*To review – for information only.*

2. MAIN BODY

1 Summary

It is over one year since the implementation of the GDPR and the DPA2018, and therefore an important juncture to review our ongoing compliance.

Under the new legislation, individuals have increased rights, organisations have additional obligations and there is a large increase in the maximum fine that can be incurred, up to a maximum of € 20 million. Furthermore, in recent weeks we have seen the regulator issue their intention to levy huge fines (£183.39million against British Airways and £99 million against Marriott International). Under the previous legislation the maximum which could be fined was £500,000.

Great Yarmouth Borough Council continue to receive customers' requests to exercise their data protection rights (including subject access requests for all their Council data). The Council has also had a complaint relating to December 2018 taken by the complainant to the Information Commissioner's Office (the regulator). As part of that complaint Emma Pheby (interim DPO) liaised with the regulator and provided a detailed account of our actions. The matter was closed, with no further action taken. It is essential that we continue to protect the Council.

Some of the recent steps taken include:

- Interim appointment of DPO (seconded from South Norfolk Council). The recruitment of a permanent DPO and the commitment to train this relevant officer.
- The recruitment of data champions from across the Council who have received additional training on data protection. The interim DPO also held a data champion meeting to discuss the practical application of the legislation across each service area and to implement further compliance steps, including requiring all service areas to complete a compliance form. Data champions cascade information across the Council, to help ensure we have a robust process and raised/ongoing awareness of the importance of data protection. The champions also coordinate the data subject and FOI requests for their service area.
- The Interim DPO has met with key services across the Council, attending both individual and team meetings, including the Housing Managers' Team meeting, Independent Team meeting, planning, IT and meeting many individual officers.
- Policies and procedures have been reviewed and revised, as required. This includes the revision of the data protection policy and the breach notification policy.
- Detailed data protection guidance has been put on the intranet and the way in which breaches are reported is now via an intranet breach notification form. Awareness has been raised across the Council via data champions, team meetings and through individual officer and at member training.

These steps help to ensure we fulfil our accountability obligations under Article 5(2) of GDPR.

As well as providing an update, this report focuses on records management for personal data (including storage, retention and deletion) and on data breaches.

Council data is both personal data and non-personal data, some information although not personal data will be commercially sensitive. This is also considered within this report (although it falls outside data protection legislation, it pertains to good information governance)
.
Personal data under the Data Protection Act 2018 and General Data Protection Regulation 2016/679 ('Data Protection Legislation') is where it identifies an individual or from which an individual is identifiable (ie not necessarily by name but using other identifying information).

1. Data Retention

2.1 Overview

Under the GDPR, Article 5(1)(e) data should be *'retained for no longer than is necessary'*. To determine what is '*necessary'* organisations need to review primary and secondary legislation, business need and good practice. It is essential that these periods are applied to ensure compliance.

Appropriate storage of commercially sensitive but non-personal data is also important, to ensure compliance with confidentiality and to protect the reputation of the Council.

The Council has in place data retention schedules across service areas. However, it is unclear as to when these have been reviewed, some have been reviewed in 2018, prior to the implementation of the new Data Protection Legislation, however others appear not to have been reviewed. It is essential that we ensure the Council retention schedules is accurate and up to date.

Under the new Data Protection Legislation, individuals have additional rights and the Council receive increased requests by customers to exercise one of their rights. If we hold data beyond the Council's agreed retention period/criteria set or we cannot justify our retention periods, individuals may complain to the Regulator (the ICO) who could take enforcement action. Furthermore, if there was a serious breach of personal data beyond the retention period, we would potentially expect to see a larger fine from the ICO.

Action**:** EP advises that all service areas are directed to follow the data retention steps at Appendix 1 to ensure we are legally compliant. It is essential to have the Heads of Service leading on this across their service areas.

2.2 Data Storage

2.2.1 Overview

Under GDPR Article 5 (1)(f) data should be '*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*.'

The GDPR recitals are clear that '*appropriate security and confidentiality of the personal data, including preventing unauthorised access to or use of personal data*.'

Furthermore, we should implement '*appropriate technical and organisational measures to ensure a level of security appropriate to risk, including… the ability to ensure ongoing confidentiality, integrity, availability*.' Some data will amount to 'special categories' of personal data (e.g. ethnic origin, political opinions, sexual orientation etc) which requires additional consideration.

2.3.2 Current Issues

Electronic data should be securely stored and only accessible to those officers who require access. Paper files should be stored in a comparably secure manner. However, some service areas storage raises concerns about legal compliance, including:

- Some HR personnel files have been stored in the Strong Room. These files include details of: home addresses, employment contracts, car registrations, bank details, copies of ID (e.g. passports), equality monitoring data (e.g. ethnicity, religion, sexual orientation – which are 'special categories' of personal data) and disciplinary issues. Any member, officer or third-party contractor who has a key fob has access to these areas. As HR's data subjects are internal the risks are higher and it is clear that additional steps should be taken by organisations (Various Claimants v VM Morrisons Supermarket [2017] EWHC 3133). This currently puts the Council at risk. However, the HR Manager discussed this matter with the interim-DPO and steps are being put in place to store this data securely within HR.
- Off-site storage – There are a number of off-site storage sites which the previous DPO referred to in a previous report in 2018. After this it was proposed there would be a review of these storage containers. It was then identified that all the data should be divided up into relevant service areas and that those service areas should then go on site with a secure waste disposal, for safe, systematic and authorised disposal. However, no further action has currently be taken and it is essential that this is dealt with. Officers have raised concerns that some of that data is thought to be data which is retained beyond the retention periods. **The Council need a clear inventory of records within these storage facilities, confirmation of security and dates of destruction assigned. on the face of it, are not currently compliant.**
- All service areas need to ensure that they are applying their retention periods/criteria and that their data is stored securely. Whilst this has been done in some areas, other service areas appear not to have undertaken a review. It is advised that Heads of Services lead on this, with support from the DPO, to ensure compliance.

2. Data Breaches

Under the Data Protection Legislation, we are now required to report relevant breaches (defined under Article 34(1) GDPR – where it is '*likely to result in a high risk to the rights and freedoms*' of a living individual/s) to the regulator. To the current DPO's best knowledge, this has not been required since implementation. We are also required to maintain an internal register of data breaches, detailing amongst other issues mitigation steps taken and why a decision was made that the breach did not require reporting to the regulator. Since EP started at GYBC she has maintained such a register, ordinarily it is best practice for a DPO to provide regular reports to the leadership team (bi-annual is suggested). This information was reported to the executive leadership team in July 2019and an overview is now provided to the Committee.

It is essential that all staff, contractors and members are aware of what to do should there be a data breach of Council data. We are required to report a relevant breach to the Regulator within 72 hours (note – this is not working hours). These 72 hours are not static, and it is important that during this time we take mitigation steps. EP has raised awareness across service areas by meeting with teams, informing the data champions at the champions meeting (for their cascade) and by providing detailed information on the Loop (https://the-loop.great-yarmouth.gov.uk/data-protection-issues) as well as reviewing and amending data sharing agreements, privacy notices, guidance, policies and processes.

Breaches provide an important learning curve whereby Officers can identify new risks and

take mitigation steps to prevent a similar breach from occurring. The lessons learnt are also shared with data champions for their cascade.

On balance the breaches which have occurred at GYBC are deemed to be relatively low level of breaches and have allowed the Council to take suitable steps which have reduced the risk of reoccurrence. It is absolutely essential that all staff, contractors, data processors and members are aware that they need to report breaches to the DPO via the intranet breach reporting form (which will be picked up in the interim-DPO's absence). The manner and level of internal reporting is reassuring. Furthermore, all officers who have reported breaches have taken the matter extremely seriously, reported very promptly and ensured that mitigation steps have been put in place. Key service areas who deal with large amounts of personal data have worked closely with the interim-DPO.

The below is a brief summary of the type of breaches which have occurred since January 2019 and actions taken.

Summary of issues	Mitigation steps taken/lessons learnt
Emails sent to an incorrect recipient	**Practical steps taken**: • Liaised with relevant staff. • reviewed the current mitigation steps and implemented auto-delay and cleansed email auto-suggest.
A customer's letter had the address of another applicant. They identified that this was due to overtyping.	**Practical steps taken**: • A blank pro forma will be used in future. • The interim-DPO has provided additional team-specific data protection training to that service area. She has also attended the managers' team meeting. • Staff were reminded of the importance of data protection and checking and this issue on each team meeting agenda.
Manual error when updating a customer's address	**Practical steps taken**: • The manager is monitoring future work and has raised awareness within the wider team. • Two letters sent for different recipients were enclosed in the same envelope – the incorrect recipient returned the mail. • Printer settings have been changed to staple multiple letters. • Furthermore, the service is seeking quotes to outsource a reputable company (frequently used by Councils) to send out these letters, given the high volumes.
Letters addressed incorrectly	Action taken: • The team were made aware of the error and reminded of the importance of data protection.

	• The manager is monitoring future work and has raised awareness with team meetings.

Complaints to the Regulator

Complaint issues:

- Outside the time limit for responding to a subject access request (received in December 2018).
- The complainant asserted excessive data collection
- Queries regarding the involvement of a third-party and clarification required as to who was the data controller and our lawful basis for processing.
- A request for safeguards/changes the organisation implemented to ensure data protection concerns are dealt with appropriately.
- Details as to the recent history of GYBC's Data Protection Officer role as at the time the previous DPO was just leaving/had left.

Action taken by the interim DPO:

- Liaised extensively with the team to gather relevant information.
- Met with the relevant third-party contractor to gather additional information.
- Reviewed the key forms and privacy notices.
- Reviewed all relevant paperwork
- Spoke with the regulator by telephone.
- Sent a detailed letter addressing each point at length.

The Regulator confirmed they were satisfied, and no further action was taken.

Appendix 1

Data Retention Schedules

Action required: All service areas must review and, as relevant, update their retention schedules, if they have not done so within the last year.
Please ensure you let the DPO know once this is done or if you have recently reviewed your retention schedule.

Which records does this apply to? Great Yarmouth Borough Council holds records in a variety of formats including electronically, paper, recorded and microfiche (and also some historic data on cards etc). Some of these records will contain personal data and/or commercially sensitive information, others will not – it applies to all these records.

The only records this does not apply to is Standard Operating Procedure records which do not ordinarily require keeping. Standard Operating Procedure records can include: out of date distribution lists, telephone message slips, trivial emails, compliment slips and some working papers leading to a final report. See the Records Management Policy for further information.

What do we need to do? It is crucial that we have a systematic and consistent way of dealing with all Council records. To help ensure this, the Council has Retention Schedules which set out how long Council records will be held across the service areas.

How long should records be held for? When considering how long Council records should be held for we should consider primary and secondary legislation, good practice and business need and ensure we have a clear and recorded justification for retention. This will include considering the Limitation Act 1980 and subject specific statutes e.g. Health & Safety at Work Act 1974. Sometimes, there is nothing which prescribes retention periods for records, so we need to consider the original purpose we collected that information for, good practice (considering any guidance) and past usage.

Where the records contain personal data, we are legal required to hold them for *no longer than is necessary* for the purpose we collected it for. We should then ensure we are clear and transparent on all Council privacy notices about how long we hold that data for.

The Information and Records Management Society previously produced a standard guide which could be adapted by Local Government, furthermore they have a Records Retention Wiki available at www.irmswiki.org.uk which can be useful (but should not be used as a definitive guide). Please contact the DPO should you have questions.

Once the retention period/criteria have been reviewed, we need to ensure they are applied. However, it is important that we do not destroy data which we may subsequently require, so need to ensure this is dealt with carefully, in line with the Records Management Policy. Please note, some records will need to be held indefinitely but we need to ensure we are clear as to why this is, store them appropriately, and are clear and transparent about retention.

It should also be noted that when considering retention periods there will be times when the ordinary retention period will not apply, for example where there is an on-going legal case or complaint.

3. FINANCIAL IMPLICATIONS

- Ensuring GYBC have adequate resources (including assigning time to relevant individuals within each service area).
- Ensuring there are resources in place to deal with the data currently stored in Council storage containers.

4. RISK IMPLICATIONS

Non-compliance with data protection legislation.

5. CONCLUSIONS

Great Yarmouth Borough Council have taken important steps by their: assignment of the interim DPO and investment in a permanent DPO; recruitment of data champions; implementation of an e-learning data protection programme; and all other steps herein.

Records management is extremely important and the approval of this policy along with the implementation of the measures advised at Appendix 1 require approval, to ensure compliance.

6. RECOMMENDATIONS

1) The publication of the Record Management Policy be approved.

2) That the updating report drafted by the Interim Data Protection Officer for the Members oversight of the Borough Council's compliance with the General Data Protection Regulation 2016/679 (EU) ('GDPR') and the Data Protection Act 2018 ('DPA2018') be noted.

Areas of consideration: e.g. does this report raise any of the following issues and if so how have these been considered/mitigated against?

Area for consideration	**Comment**
Monitoring Officer Consultation:	No – already involved in discussions in this regard.
Section 151 Officer Consultation:	No
Existing Council Policies:	Updating relevant policies to refer to the new Record Management Policy.
Financial Implications (including VAT and tax):	
Legal Implications (including human rights):	No
Risk Implications:	No risks reduced by implementation.
Equality Issues/EQIA assessment:	None presented.

Crime & Disorder:	No
Every Child Matters:	

Great Yarmouth Borough Council

RECORDS MANAGEMENT POLICY

Author	Emma Pheby
Date	July 2019
Last Review Date	July 2019
Review Changes	
Version	1.0 (Also replaces previous GDPR Policy – see also Data Protection Policy)
Document Status	Draft

1. Introduction

This Records Management Policy sets out Great Yarmouth Borough Council's commitment to ensuring a systematic, lawful and authorised way of maintaining, storing, sharing, disposing and otherwise processing all its records.

This Policy is in place in accordance with recommendations in the Information Commissioner's Section 46 Records Management Code of Practice which sets out Guidance for public authorities. This policy recognises that Council information and records are key corporate assets.

Retention Guidelines are an important part of records management based on relevant legislation (including the Limitation Act 1980 and subject specific statutes e.g. Health and Safety at Work Act 1974), good practice and business need. Great Yarmouth Borough Council regularly review their Retention Guidelines in consideration of the Records Management Society of Great Britain.

Adherence to this policy will ensure that records are accurate, reliable and accessible and will further ensure that the necessary processes are in place to:

- Ensure we operate effectively as a Local Council.
- Ensure we are compliant with Data Protection Legislation (defined at paragraph 3) and all other applicable legislation.
- Provide an open and transparent service.
- Carry out our business in a systematic, consistent and organised manner.
- Ensure data is stored securely and kept for no longer than is necessary.
- Carry out disposal in an authorised and appropriate manner.
- Ensure cost effectiveness is considered.
- Provide an audit trail to meet business, regulatory and legal requirements.

This Records Management Policy has been produced to assist officers within Great Yarmouth Borough Council with the management, retention, storage, sharing and disposal of Council records.

2. Scope

This Policy applies to Council records in all formats, including online, paper, microfiche and any historically created record format (e.g. card or register).

This policy applies to:

- All staff (including temporary and permanent employees, agency and casual staff)
- Elected Members
- Third parties processing data on behalf of the Council, including contracted suppliers or partners.

3. Statutory and Regulatory Environment

General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and all implementing/updating legislation– 'Data Protection Legislation'

Freedom of Information Act 2000

The Privacy and Electronic Communications (EC Directive) Regulations 2003

Section 46 Code of Practice – The Information Commissioner's Office

The Environmental Information Regulations 2004

4. Definitions

4.1 Personal Data

'Personal Data' means 'any information relating to an **identified** or **identifiable natural person**; an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.2 Sensitive Personal Data

'Sensitive Personal Data' means 'personal data revealing **racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, or **trade union membership**, and the processing of **genetic** data, **biometric** data for the purpose of uniquely identifying a natural person, data concerning **health** or data concerning a **natural person's sex life** or **sexual orientation** shall be prohibited'.

4.3 Non-Personal Data

'Non-Personal Data' means data from which an individual is not identified or identifiable. Fully anonymised data which fulfils this description will also be Non-Personal Data.

4.4 Records

'Records' and Documents' applies to Council records in all formats, including electronic, online, paper, microfiche, photograph and any historically created record format (e.g. card or register). It applies to both Personal Data, Sensitive Personal Data and Non-Personal Data.

4.5 Data Protection Legislation

Data Protection Legislation means the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 and any national implementing laws and secondary legislation, as amended or updated from time to time, in the UK, and any other successor legislation and all other applicable data protection law.

5. Responsibility

Record management responsibilities are provided across the Council as set out below:

Senior Information Risk Owner (SIRO)	The SIRO is responsible for overall risk management of records.
Data Protection Officer	The DPO liaises with the ICO, as required, and oversees compliance of Data Protection Legislation. Where the DPO is not available/not working, the Corporate Services Manager.
Heads of Services – Information Asset Owners	The Directors/Heads of Service are the Information Asset Owners (IAOs) for their services. They will oversee delegated responsibilities.

All employees, contractors, third parties and partners who process Council records have a role in ensuring good Records Management of Council data, and in complying with this policy.

6. Retention

6.1 In compliance with Data Protection Legislation, Personal Data will be retained for '*no longer than is **necessary** for the purposes for which the personal data are processed'*. To determine what has been deemed as necessary please refer to the Retention Guidelines which are an appendices to this Policy. The Retention Guidelines provide details of all the Council's records both Personal and Non-Personal Data.

Retention periods have been set in accordance with primary or second legislation, or where there is not a legal requirement, they have been set in accordance with business need or good practice.

As a Local Authority we may also identify a need to retain Documents of historical value.

Where records are authorised for destruction they should be destroyed in accordance with paragraph nine.

6.2 <u>Standard Operating Procedure</u>

Standard operating records do not ordinarily need to be kept and can be destroyed in line with the disposal guidelines below. Standard Operating Procedure records can include: **working papers leading to a final report, out of date distribution lists, telephone message slips, trivial emails, compliment slips and telephone message slips (this is a non-exhaustive list**).

Council documents, which are not Standard Operating Procedure records, will be retained in accordance with the Council's Retention Schedules.

6.3 Scanned copies - Where you have scanned original copies of documents and we do not need to keep an original copy you must ensure that the scanned copy is clear and legible prior to disposal. In some circumstances, an original copy will need to be safely and securely stored. The Inland Revenue and Customs and Revenues prescribe the retention of original paperwork in some circumstances. Law Society Guidance also provides information on the retention of some original documentations, such as deeds or guarantees.

Service Managers are responsible for:

i) Ensuring that scanned documents are legible and provide a true copy of the original.
ii) Ensuring that scanned documents are retained in accordance with the document retention schedules as detailed in Appendix 1.
iii) Ensuring that scanned documents can be located and retrieved promptly when required for either:
    - Operational purposes
    - A Subject Access Request or other exercise of a data subject's rights under Data Protection Legislation.
    - A request under the Freedom of Information Act 2000
    - Legal Proceedings

6.4 Document Retention and Disposal Protocol

6.4.1 Each Head of Service is the assigned Information Asset Owner. They must ensure that they have in place an adequate system for documenting the retention of records within their service. This system should take into account the legislative and regulatory environment in which they work.

6.4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

- Facilitate an audit or examination to those authorised to do so
- Protect the rights of the Council, its residents, contractors and clients and any other persons affected by its actions.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

6.4.3 To facilitate 6.4.2 the following principles should be adopted:

a) Records created and maintained should be arranged in a record keeping system ensuring ownership of these records that will enable the Council to obtain the benefit from the quick and easy retrieval of information.

b) Record systems utilised within services whether paper or electronic, should include a set of rules for referencing, titling, indexing, and if appropriate, security

marking documents and records. These should be easily understood and enable the efficient retrieval of information.

c) The movement and location of records should be controlled to ensure that a record can easily be retrieved at any time and that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

d) Storage accommodation for current records should be clean and systematic, to prevent damage to the records and to ensure accessibility. Equipment used for current records should provide storage, which is safe from unauthorised access, meets fire regulations, but allowing maximum accessibility to authorised officers when required.

e) Documents that are no longer required for operational purpose but still require retention should preferably be placed in a designated records centre.

f) Services should ensure that a contingency or recovery plan is in place to provide protection for records, which are vital to the continued functioning of the Council.

g) A system should be in place to ensure that where a member of staff leaves, changes role, or is absent, that Records remain accessible to those who will require access. Information Asset Owners should ensure that a suitable system is in place.

7. Storage

The Council hold records in a variety of formats, including in electronic, paper, microfiche and video recording formats; all of which will be stored in a suitable manner taking account of the type of records.

7.1 Paper storage:

Paper documentation will be stored appropriately according to the level of security required. The Council office has controlled access, which provides security for all on-site Council documentation. Furthermore the Council run a Clear Desk Policy.

Risks will be considered and personal or sensitive data will have the appropriate additional security measures, which may include storing personal data in a lockable cabinet, in a lockable drawer or in a secure archiving storage facility.

7.2 Electronic storage:

A back-up of all electronic Council data is kept in accordance with the Council's IT Back-Up Policy. The Council have robust electronic information security and technical measures in place which are regularly reviewed and updated.

The following issues must be considered when storing documents electronically:

STORAGE QUESTIONS	STEPS TO CONSIDER
1. Who has access to the personal data, sensitive personal data or	Ensure that access is controlled and only limited to those who need access.

confidential documentation?	Ensure that should you be absent or leave your role that the records do not become inaccessible.
2. What technical and security measures are in place?	Ensure that there are sufficient technical and security measures in place to prevent a breach.

8. Data Sharing

Where data is transferred to another organisation we must take steps to ensure the safety of the records during the transportation or transmission process. This should include:

- Password protection – the password should, wherever possible, convey a different medium (For example do not email password details and then also email the password protected data)
- Encryption
- Use of secure email servers
- Minimisation of personal/sensitive personal data to what is needed only.
- Sending data by secure online portals with limited access

8.1 Data Processors: Where the Council have contracted a third-party supplier to process Council data on our behalf we must take steps to ensure that the Data Processor complies with security and technical measures to protect this document in line with Data Protection Legislation. These steps include relevant clauses being inserted into our contracts as required under Article 28 General Data Protection Regulation 2016/679. You will also need to undertake due diligence by asking appropriate questions regarding security and technical measures taken where suppliers will be processing Council personal data.

An example of data processors may be where we contract a third party to provide and administer an IT system to our instruction on which we store our customers personal data.

8.2 Systematic Data Sharing with Data Controllers: Where we share personal data systematically with other Data Controllers we should have a Data Sharing Agreements in place which set out the details of the data sharing. Where we share personal data, we will ensure we are compliant with Data Protection Legislation.

Some examples of where may require a data sharing agreement includes where we share personal data with another Local Authority for election purposes or where we share data with a Housing Association or where we share data to deliver the Neighbourhoods that Work project.

9. Disposal

9.1 Where records have come to the end of their retention period and are to be destroyed they must be destroyed appropriately.

Disposal should be authorised and systematic. This will involve ensuring that your team have a system in place for the regular review of documents which is authorised by a relevant manager or Head of Service. Where Personal Data or other Non-Personal but commercial sensitive personal data is destroyed it will be safely and secure disposed of using confidential waste units.

Furthermore, in some cases, a record of this destruction should be made. To decide whether to record evidence of its destruction there should be a consideration of 1) whether there is a business need to record the presence of those previous records 2) an assessment of the risk should destruction of that particular record be questioned. The record could include the disposal class, a date range and confirmation that this disposal was authorised, evidence/details of how the disposal occurred. The record of destruction should provide enough detail to identify which records have been destroyed but will not ordinarily contain Personal Data.

These measures are to safeguard against a proposition that records were eliminated to avoid disclosing them.[1] Therefore, when appropriate destruction should be documented in line with legislation and appropriate authorisation.

9.2 As a Local Authority we have an obligation to have a robust back-up system to ensure electronic data which we need to retain is not lost. Please see the IT Back-up Policy for more details.

9.3 When disposing of records the following steps must be considered:

Has disposal been authorised?	Ensure that the disposal has been authorised and that it is done in compliance with the Retention Guidelines, and that an exception does not apply (e.g. there is a legal case or complaint pending).
Is retention required to fulfil legislation or regulatory requirements?	Consider primary and secondary legislation and good practice guidance.
Is there a current, or potential, dispute or legal challenge?	Our decisions regarding retention will ordinarily take account of the Limitation Act. If there is any ongoing legal case or other dispute, or a potential for one, then we should ensure this data is retained.
Do the records contain any personal data, sensitive personal data or	If yes, ensure safe destruction by shredding or in confidential waste bins.

[1] Code of Practice on Records Management issued under s46 Freedom of Information Act 2000; The National Archives, Record Management Policy - Guide

confidential data?	Failure to adhere to this will breach Data Protection Legislation. We must ensure that destroyed data is 'virtually impossible to retrieve'.
Do we need to keep a record of the documentation destroyed?	Consider this in line with 9.1

10. Review

This Policy will be reviewed within three years and earlier if appropriate. This Policy will be made readily available on the Council's intranet service to ensure that it is easily accessible.