EARLEY TOWN COUNCIL

DATA PROTECTION POLICY

Our Commitment

The processing of personal information is important to us and the Council understands the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

The Council will only collect, use and hold personal data about individuals for the purposes of carrying out our statutory obligations, delivering services and meeting the needs of individuals. This includes, service users, members of the public, current, past and prospective employees, Members of the Council, stakeholders and other local authorities, public bodies or law enforcement agencies.

The Town Council will only keep data for as long as it is necessary to do so, as per our Retention Schedule.

Our Objectives

In order to comply with the requirements of the Data Protection Act 2018, including the UK General Data Protection Regulation, the Council will ensure that:

- Personal data is collected, used and held, lawfully and processed for the purpose it is intended.
- Regular data sharing with external partners and other relevant agencies will be subject to information sharing agreements and will only be entered into with third party under a duty of confidentiality and they will be obliged to implement appropriate measures to ensure data security.
- External agencies undertaking any data processing on behalf of the Council will be required to demonstrate compliance with the Data Protection Act 2018 and will require measures to be in place to protect personal data.
- Staff are aware of their responsibilities when processing personal information.
- Training is provided to ensure that those handling personal data are trained appropriately.
- The Deputy Town Clerk is the appointed person who has knowledge in data protection compliance and who is a point of contact for all queries.
- Subject Access rights can be fully exercised and will be dealt with promptly.
- Any new projects being implemented that involves personal data to be subject to a Data Protection Impact Assessment (DPIA).
- We will review and update this policy, procedures and guidance for Council employees and Members on a regular basis.

We are required by law to share or make available some of the personal data we collect and hold. This information may be shared for a number of reasons to safeguard public funds and for the prevention and detection of fraud, and for the prevention and detection of crime. For more details on this please read our General Privacy Notice.

We will fully comply with the requirements of the Data Protection Act 2018 and are registered as a data controller with the Information Commissioner’s Office. Our registration number is Z7740800.

Meeting our Objectives

In order to meet our objectives we will ensure that the following are always considered and that appropriate controls and procedures are in place to ensure compliance with the Data Protection Act 2018.

Collecting and Processing Personal Data

- When we collect personal data we will ensure that where required, we make individuals aware that their information is being collected, the purpose for collecting the data and whether it will be shared with any third parties. This will be done through the use of privacy notices.
- No new purpose for processing data will take place until the Information Commissioner's Office has been notified of the relevant new purpose and the data subjects have been informed and consent has been sought where required.

Data Security

- Council employees and members must report any suspected data breaches to the responsible officer for investigation and where necessary a responsible officer will notify the Information Commissioner's Office
- Council employees and members must use appropriate levels of security to store or share personal data. Training will be provided to employees and members
- When undertaking new projects involving personal data, a Data Protection Impact Assessment (DPIA) will be carried out by the Project Manager and reviewed by a responsible officer in order to assess any potential privacy risks.

An Information Asset Register will be maintained by the Town Clerk & Deputy Town Clerk identifying:

- all personal data held.
- where it is held.
- how it is processed.
- who has access to it.

Personal data will not be shared with a third-party organisation without a valid reason and where required an individual will be notified that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, consent from the individuals concerned must be obtained.

When personal data is to be shared regularly with a third party, a Data Sharing Agreement must be implemented.

Any data sharing will also take into consideration:

- the statutory basis of the proposed information sharing.
- whether the sharing is justified.
- how to ensure the security of the information being shared.

Data Access

- Our employees and members will have access to personal data only where it is a requirement of their job role.
- All data subjects have a right of access to their own personal data and further detail on how to request or access personal data held by us can be found on our website.
- Our employees and members are aware of what to do when requests for information are made under the Data Protection Act 2018.
- Our employees and members are made aware that in the event of a Subject Access Request being received, their emails may be searched and relevant content disclosed.
- A Subject Access Request will be acknowledged to the data subject within 24 hours, with the final response and disclosure of information (subject to exemptions) within 40 calendar days.
- A Subject Access Request will not be responded to until the individual requesting the information can verify their identity.
- Third party personal data will not be released when responding to a Subject Access Request, unless consent has been obtained, it is required to be released by law, or it is deemed reasonable to release.

Data Protection Officer (DPO)

Earley Town Council's Data Protection Officer is the Deputy Town Clerk who is responsible for ensuring the council's compliance with data protection legislation and to inform and advise on the council's data protection obligations.

Compliance with this Policy

This Policy applies to all council employees, members and all individuals or organisations acting on behalf of the council.

Date of adoption: xx July 2022

Date of review: July 2024

EARLEY TOWN COUNCIL

INFORMATION SECURITY POLICY

Introduction

This policy is set out to ensure the appropriate use of council IT equipment and computer systems and to safeguard the security of information and to ensure that staff understand what is and is not permitted.

Scope

This policy covers the computer systems and technology systems used by staff when carrying out council business.

Computer Access

Access to computer IT systems is controlled by user IDs and passwords. All user IDs and passwords have been assigned to individual staff members and staff members are responsible for ensuring that these details are used for the purpose they are intended.

Staff must: -

- Log out if they are away from their desk.
- Not carry out any changes to IT systems without authorisation from the council's IT service providers.
- Not attempt to access data that they are not authorised to access.
- Not connect unauthorised devices/personal devices.
- Not store council information on unauthorised equipment/devices.
- Not transfer data to a person/s outside the council unless authorised to do so.
- Notify the Town Clerk if a password is changed.

Emails

Staff issued with email accounts are intended for council business use only. Personal use is permitted but only where it does not affect a staff member's work performance, is not detrimental to the council and does not breach any terms of employment or other legal obligations. Emails should be treated the same as any other form of documentation.

The following is considered unacceptable use of emails: -

- Forwarding confidential council emails/information to external emails.
- Distributing material which is illegal.
- Distributing material which is discriminatory, offensive or abusive.

All individuals are accountable for their actions when using email systems.

Staff should delete or archive emails on a regular basis when no longer required. In accordance with the Council's Retention Schedule, emails should only be kept for a certain period of time.

Staff must be aware of spam and phishing emails and should not reply to them and inform the council's IT service provider of any suspicious emails.

Emails sent by staff must have the council's appropriate disclaimer relating to the use of the information contained within the email.

Internet

Internet usage is intended for business use only. Personal use of the internet is permitted but only where it does not affect a staff member's work performance, is not detrimental to the council and does not breach any terms of employment or other legal obligations.

The following is considered unacceptable use of the internet: -

- Downloading unauthorised software or copyright material.
- Use of personal social media.
- Sending of offensive material.
- Visiting sites that contain pornographic, obscene, hateful or illegal material.
- To reveal confidential council information.
- To introduce viruses/malicious software onto the council's computer systems.

Telephone Systems

The telephone system is for council business only and staff should not use it to make personal calls unless they have obtained authorisation.

Mobile Phones

Staff who have been issued with a work mobile phone should only use their phone for council business. Staff must take care when displaying information on their phone and ensure that they take precautionary measures so not to disclose or display personal data or confidential information when using their phone in public.

Protecting Information

All staff must ensure that they reduce the risk of unauthorised access, loss of personal data and data breaches of council information by: -

- Logging off of their computer when not at their desk.
- Ensuring confidential information/personal data is not left unattended or is locked away.
- Not leaving confidential information/personal data on printers.
- Protecting access to mobiles phone with passcodes.
- Shredding any paper copies containing confidential information/personal data in accordance with the Council's Retention Schedule.

Remote Working

This policy is applicable to any member of staff when remote working.

Personal Devices

Personal devices are not to be connected to the council's computer systems unless authorised by the Town Clerk.

Personal devices are considered to be: -

- Laptops
- Tablets
- Smart Phones
- Portable Storage, e.g., hard drives, memory sticks, data cards
- Cameras

Removeable Storage

The use of council removable storage is permitted and is the responsibility of the person operating the storage. Removeable storage must be used for council business only and when the data on the storage is no longer required, it should be deleted.

Removable storage is considered to be: -

Memory Cards
USB sticks
Mobile devices – mobile phone, cameras etc
DVDs/CDs

Monitoring

The Council recognises the importance of an individual staff privacy but has to balance this against the requirement to protect information and preserve the integrity of the council. The council may on occasions carry out monitoring of the use of the council's IT systems.

The reasons for monitoring are: -

- To ensure staff are complying with this policy.
- To detect any inappropriate behaviour or communication.
- To ensure that personal data and sensitive information is being processed correctly.

The ways in which monitoring can be carried out are: -

- Physical inspection of computers and desks.
- Inspection of call logs
- Inspection of internet activity.
- Inspection of email activity.
- Inspection of telephone communication.

Breach of Policy

A breach of this policy could lead to disciplinary action being taken.

Date of adoption: xx July 2022

Date of review: July 2024

EARLEY TOWN COUNCIL

INFORMATION BREACH POLICY

Introduction

This policy demonstrates that the Council is complying to the Data Protection Act 2018, including the UK General Data Protection Regulation to ensure that personal data breaches are dealt with appropriately and in a timely manner.

What is a personal data breach?

The Information Commissioner's Office (ICO) defines a data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed ".*

Risk Assessment

A risk assessment has been undertaken which identifies the various functions of the Council and information collected to help manage breaches on a day-to-day basis. This is documented in the council's Information Asset Risk Register.

Reporting a data breach

When an officer or councillor is aware that a data breach has occurred, they must report this immediately to the Town Clerk. If outside normal working hours, then as soon as possible.

Investigating a data breach

It will be the responsibility of the Deputy Town Clerk, as the Data Protection Officer to enter the details of the breach onto a Personal Data Breach Form on the ICO's website and to carry out a thorough investigation into the breach.

The investigation will assess the risks associated with the breach in relation to the potential consequences for individuals, the level of severity of those consequences and how likely they are to happen.

The investigation will consider the following: -

- The type of information involved.
- Was it human error or a system issue?
- The sensitivity of the information.
- The protections that are in place (e.g., passwords, encryptions).
- What has happened to the data (e.g., lost, stolen, disclosed).
- Whether the data could be used for illegal purposes.
- The individuals (data subjects) who will be affected, the number of individuals affected and the potential effects on those individuals.
- Whether there are any wider consequences.
- If there is high risk to adversely affecting individuals' rights and freedoms.
- Whether the personal data can be recovered to limit the damage the breach could cause.
- Who needs to be notified for immediate containment?
- Suitable action to be taken to resolve the incident.

Reporting a breach to the ICO

Not every breach needs to be reported to the ICO and the ICO's Self-Assessment can help determine whether a breach needs to be report to them, this can be carried out at: - https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

The ICO must be informed of a breach if the breach: -

- will result in the risk to the rights and freedoms of an individual.
- will result in the risk of damage to reputation, financial implications, confidentiality loss, discrimination, social/economic disadvantage to an individual.

A breach must be reported to the ICO as soon as possible and no later than 72 hours of becoming aware of the breach, even if all the details of the breach are not known.

To report a breach to the ICO a Personal Data Breach Reporting Form must be completed which can be found at: - https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ and emailed to: - icocasework@ico.org.uk with the words "Personal Data Breach Notification" in the subject line.

Failure to report a breach to the ICO

Failure to notify the ICO of a breach when required to do so can result in a fine, along with the ICO's corrective powers.

Notifying affected individuals of a breach

Any individuals whose personal data has been affected by a breach and where it is considered likely to result in a high risk of adversely affecting an individual's rights and freedoms must be informed of the breach.

The following information must be provided to an individual affected: -

- How and when the breach occurred.
- The data involved.
- A description of the likely consequences.
- The actions taken or proposed to deal with the breach and to mitigate adverse effects.
- Steps the individual can take to protect themselves, such as password reset, looking out for phising emails of fraudulent activity on accounts.
- The contact details of the person dealing with the breach.

Evaluation

Once the breach has been contained, a full review should be carried to consider the causes of the breach, the effectiveness of the response in limiting adverse effects and to consider whether systems, policies or procedures need to be changed and whether further training is required.

Further information: -
https://ico.org.uk/for-organisations/report-a-breach/

Date of adoption: xx July 2022
Date of review: July 2024

EARLEY TOWN COUNCIL

WEBSITE PRIVACY & COOKIE POLICY

This policy applies to the content of the Town Council's website only (https://www.earley-tc.gov.uk/) and not to any external sites that we provide links to, including the Town Council's Facebook/Twitter page.

Privacy

The Council does not currently collect personal information from members of the public through our website site, as we do not have a "Contact Us" facility on our website.

We do use Google Analytics to help us understand how our customers use the site and you can read more about how Google uses your Personal Information at:
https://www.google.com/intl/en/policies/privacy/

You can also opt-out of Google Analytics here: https://tools.google.com/dlpage/gaoptout

Use of Cookies

Cookies are small text files which are placed on your computer or mobile device by websites that you visit. Cookies are used in order to make websites work, provide information to site owners and to display content that is personalised to users based on their previous internet activity.

There are 2 different types of cookie which can be placed in your browser by a website:

Session cookies – are used for the timeframe you use the website, which are then deleted when you close your web browser. A new cookie would then be placed in your browser if you were to visit the same website again.

Persistent cookies - remain in your browser once you have left the site and closed your browser. The next time you visit the site the cookie will be used to make the website work as it did at the time of your previous visit. Persistent cookies will expire if the website is not visited again within a certain timeframe.

Examples of cookies can be:

- The storing of information to personalise a website to your requirements
- A website selling items uses cookies to record items you have in a shopping basket
- To record and analyse users activity on a website, for example what pages have been viewed

Cookies on This Website

We use standard cookies on our website. If you have any questions about the way cookies are used, or how you may be affected please contact us.

Managing Cookies on Your PC

You can choose to block cookies that are set by our website, however by doing this it may mean that some parts of the website will not work correctly.

Date of adoption: xx July 2022

Date of review: July 2024

EARLEY TOWN COUNCIL

FREEDOM OF INFORMATION POLICY

Introduction

This policy sets out how Earley Town Council will provide information to applicants who request information in writing from the council under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Scope

The Freedom of Information Act 2000 gives a general right of access to all types of recorded information held by the council. The Act gives the public greater access to information about the functions of the council. This policy should be read in conjunction with the council's Data Protection Policy and Freedom of Information Guidance.

The Council's Model Publication Scheme

The council has an adopted Model Publication Scheme which allows members of the public to view or obtain information held by the Town Council.

The ways in in which to obtain information are as follow: -

Website

The Town Council's website holds routine information which the council publishes, so individuals should first visit the council's website to see if the information they require is available there. https://www.earley-tc.gov.uk/

Request information

Submit a Freedom of Information request or EIR request in writing to: -
Town Clerk
Earley Town Council
Radstock House, Council Offices
Radstock Lane
Earley
Reading
RG6 5UL

Or by email to: townclerk@earley-tc.gov.uk

Requests must include name of requester, address for correspondence to be sent to, which can be an email address and details of the information being requested.

Date of adoption: xx July 2022

Date of review: July 2024

EARLEY TOWN COUNCIL

SUBJECT ACCESS REQUEST POLICY

Introduction

Under the General Data Protection Regulations (GDPR), an individual, as a data subject has a right to know what information the Council, as a data controller holds on them, why their data is being processed and whether it has been or will be shared with a third party and that their data is being processed lawfully. An individual can request this information as a Subject Access Request.

Responsibilities

It is the Council's responsibility to ensure that this policy is followed when dealing with a Subject Access Request. Data subjects are informed of their rights to access data, which is documented in the Council's Privacy Notice.

The Council's Subject to Access Request Guidance should be read in conjunction with this policy.

Subject Access Request (SAR)

- A SAR can be made verbally or made in writing, either by letter, email or social media. The request does not have to state it is a SAR but must be dealt with as one.

- A third party can make a SAR on behalf of another person if that person is entitled to act on behalf of the individual. It is the responsibility of the third party to provide evidence of their authority.

- A child can make a SAR for their own personal information if they are competent to do so dependent on the level of understanding of the child and not acting against their own best interests. A child can authorise someone else to act on their behalf such as a parent another adult or a representative.

- Whilst the Council does have a SAR Form, a data subject does not have to complete a request form, as GDPR determines a written request as sufficient.

- The Council must respond to a SAR within one month of receipt of a request. This time can be extended by 2 months if the request is complex of if a number of requests have been received from the same individual.

- The Council will perform a reasonable search for the requested information, however, is not required to conduct searches that are unreasonable or disproportionate to the importance of providing access to the information. Searches will be carried out of emails, including archived emails, word documents, spreadsheets, databases, filing systems, computer systems, memory sticks, CDs, DVDs and recordings.

- The Council can only refuse a request if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

- Any information will be provided to the data subject in a manner that is easy to understand and securely.

- The Council cannot charge for providing the requested information, unless legislation permits that a reasonable fee can be charged.

Subject Access Request Rights

The main legislative measures that give rights of access to records include:

The Data Protection Act 2018 (DPA) – rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf.

The General Data Protection Regulations (GDPR) - Individuals have the right, under the General Data Protection Regulation (EU) 2016/679 (Articles 12 and 15) to request access to, or a copy of, information an organisation holds about them.

Complaints

Should a data subject make a complaint about the handling of their SAR, this must be dealt with in accordance with the Council's Complaint Process and the requestor should be advised that they may also complain to the Information Commissioners Officer at https://ico.org.uk/global/contact-us or at the Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or telephone 0303 123 1113, if they remain unhappy with the outcome of their complaint.

Compliance with this Policy

This Policy applies to all Council employees, members and all individuals or organisations acting on behalf of the Council.

Date of adoption: xx July 2022

Date of review: July 2024

EARLEY TOWN COUNCIL

RETENTION OF RECORDS & DISPOSAL POLICY

Introduction

Earley Town Council recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the council.

The council accumulates a vast amount of information and data during the course of its daily activities and this includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.

Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.

This policy and the Council's Retention Schedule identifies the council's obligations for retaining and destroying information in accordance with various legislations and best practice guidance.

Records created and maintained by the council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the council's transactions and are necessary to ensure it can demonstrate accountability.

It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the council.

In contrast to the above the council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

Scope

This policy applies to all records created, received or maintained by Earley Town Council in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by Earley Town Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activates.

Objective

The objective of this policy is to provide a working framework to determine which documents are:-

- Retained and for how long
- Disposed of information

There are some records that do not need to be kept or that are routinely destroyed as part of the council business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:

- With compliments' slips.
- Catalogues and trade journals.
- Non-acceptance of invitations.
- Trivial electronic mail messages that are not related to Council business.
- Requests for information such as maps, plans or advertising material.
- Out of date distribution lists.

Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed. Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations

Responsibilities

Earley Town Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Town Clerk. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

Individual staff and employees have a responsibility to ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with Earley Town Council's records management guidelines. An annual review of documentation should be carried out to determine whether to retain or dispose of documents and that any unnecessary documentation being held is disposed of under the Data Protection Act 2018. All employees should be fully aware of the Council's Retention Schedule.

Document Retention Protocol

Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.

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 of the business by anyone so authorised.
- Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
- Verify individual consent to record, manage and record disposal of their personal data.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

To facilitate this the following principles should be adopted:

- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
- Documents that are no longer required for operational purposes but need retaining should be archived appropriately.

Appendix A: Retention Schedule is guidance on the recommended minimum retention periods for specific classes of documents and records. This schedule has been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

Document Disposal Protocol

Documents should only be disposed of if reviewed in accordance with the following:

- Is retention required to fulfil statutory or other regulatory requirements?
- Is retention required to meet the operational needs of the service?
- Is retention required to evidence events in the case of dispute?
- Is retention required because the document or record is of historic interest or intrinsic value?

When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

Documents can be disposed of by any of the following methods:

- Non-confidential records to be placed in wastepaper bin or recycling bin for disposal.
- Confidential records or records giving personal information to be shredded.
- Computer records to be deleted.
- Where documents are of historical interested it may be appropriate to transfer the records to an external body such as the local Records Office.

The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the council being prosecuted under the UK General Data Protection Regulations.
- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
- Where documents are of historical interest it may be appropriate that they are transferred to the local Records Office.
- Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

Records should be maintained of high importance disposals such as financial or HR records etc.

These records should contain the following information:

- The name of the document destroyed.
- The date the document was destroyed.
- Person authorising the disposal.
- The method of disposal.

Data Protection Act 1998 – Obligation to Dispose of Certain Data

The Data Protection Act 1998 requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. The Data Protection Act defines personal information as "*data that relates to a living individual who can be identified"* from the data, or from those data and other information, which is in the possession of, or is likely to come into the possession of the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the council or other person in respect of the individual.

The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met. The council is responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations being:

- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall only be collected for specific legitimate purposes and not processed in a manner incompatible with those purposes.
- Personal data shall be adequate, relevant, but not excessive.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Personal data shall be kept secure.

External storage providers or archivists that are holding council documents must also comply with the above principles of the General Data Protection Regulations.

Scanning of Documents

In general, once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs. As a general rule hard copies of scanned documents should be retained for three months after scanning and then disposed of.

Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

Review of Document Retention

It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the Code of Practice on the Management of Records issued by the Lord Chancellor).

This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:

- Local Council Administration, Charles Arnold-Baker, 910h edition, Chapter 11
- Local Government Act 1972, sections 225 – 229, section 234
- SLCC Advice Note 316 Retaining Important Documents
- SLCC Clerks' Manual: Storing Books and Documents
- Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000

Retention Schedule

Please see Appendix A Retention Schedule document which is updated regularly in accordance with any changes to legal requirements.

Date of adoption: xx July 2022

Date of review: July 2024