



Surrey Heath Borough Council
Surrey Heath House
Knoll Road
Camberley
Surrey GU15 3HD
Telephone: (01276) 707100
Facsimile: (01276) 707177
DX: 32722 Camberley
Web Site: www.surreyheath.gov.uk

Department: Democratic Services
Division: Corporate
Please ask for: Rachel Whillis
Direct Tel: 01276 707319
E-Mail: democratic.services@surreyheath.gov.uk

Monday, 19 April 2021

To: The Members of the **Employment Committee**
(Councillors: Colin Dougan (Chairman), Cliff Betton (Vice Chairman), Sharon Galliford, Josephine Hawkins, Rebecca Jennings-Evans, Alan McClafferty, Sashi Mylvaganam, Graham Tapper and Victoria Wheeler)

In accordance with the Substitute Protocol at Part 4 of the Constitution, Members who are unable to attend this meeting should give their apologies and arrange for one of the appointed substitutes, as listed below, to attend. Members should also inform their group leader of the arrangements made.

Substitutes: Councillors Peter Barnett, Rodney Bates, Paul Deach, Adrian Page, Morgan Rise and Kristian Wrenn

Dear Councillor,

A meeting of the **Employment Committee** will be held virtually on **Wednesday, 28 April 2021 at 5.00 pm**. The agenda will be set out as below.

Please note that this meeting will be recorded and live streamed on <https://www.youtube.com/user/SurreyHeathBC>

Yours sincerely

Damian Roberts

Chief Executive

AGENDA

Pages

Part 1 (Public)

1	Apologies for Absence	-
2	Minutes	3 - 8
	To confirm and sign the minutes of the meeting held on 25 March 2021 (copy attached).	
3	Declarations of Interest	-

Members are invited to declare any interests they may have with respect to matters which are to be considered at this meeting. Members who consider they may have an interest are invited to consult the Monitoring Officer or the Democratic Services Officer prior to the meeting.

4 Records Management Policy 9 - 20

5 Exclusion of Press and Public -

The Committee is advised to RESOLVE that, under Section 100A(4) of the Local Government Act 1972 (as amended), the public be excluded from the meeting for the following items of business on the ground that they involve the likely disclosure of exempt information as defined in the paragraphs of Part 1 of Schedule 12A of the Act, as set out below:

<u>Item</u>	<u>Paragraph(s)</u>
6	1
7	1
8	1
Part 2 (Exempt)	

6 Exempt Minutes -

To confirm and sign the exempt minutes of the meeting held on 25 March 2021 (copy to be circulated separately).

7 HR Matter -

Report to be circulated separately.

8 Review of Exempt Items -

To review those items or parts thereof which can be released as information available to the public.

**Minutes of a Meeting of the
Employment Committee held on 25
March 2021**

- Cllr Colin Dougan (Chairman)
+ Cllr Cliff Betton (Vice Chairman) (in the chair)

+ Cllr Sharon Galliford	+ Cllr Sashi Mylvaganam
+ Cllr Josephine Hawkins	+ Cllr Graham Tapper
+ Cllr Rebecca Jennings-Evans	+ Cllr Victoria Wheeler
+ Cllr Alan McClafferty	

+ Present
- Apologies for absence presented

Members in Attendance: Cllr Rodney Bates, Cllr David Mansfield, Cllr Valerie White.

34/EC Minutes

The minutes of the meeting held on 28 January 2021 were agreed and would be signed by the Chairman at the earliest opportunity.

35/EC Information Security Policy

The Committee was informed that the Information Security Policy set the framework for protecting and securing the Council's information assets. The Policy, which had last been reviewed in March 2020, comprised a number separate documents which covered the rules and guidance to be applied by staff. A further review had been carried out and the recommended changes were as set out at Annex A to the agenda report. In addition to the recommended changes, it was agreed that Paragraph 3 of the Policy would be amended to state that staff must attend scheduled training on an annual basis.

RESOLVED that the revised Information Security Policy, as set out at Annex A to the agenda report, as amended, be agreed.

36/EC Data Protection Policy

The Data Protection Policy set out the framework for compliance with the requirements of the Data Protection legislation and provided guidance to all council staff to help them understand the importance of their role in maintaining the security and confidentiality of personal data. The Data Protection Policy had been reviewed and the recommended changes were set out at Annex A to the agenda report.

The Committee considered paragraph 1.5 of the Policy which referred to ensuring that, where work was outsourced, the companies used complied with the same standards as would be expected if the work was completed by the Council. This paragraph had been inserted following review by the Joint Staff Consultative

Group and Members recognised that, as the wording was currently aspirational, it should be further reviewed.

RESOLVED that

- (i) subject to the revision of paragraph 1.5, the revised Data Protection Policy, as set out at Annex A to the agenda report, be agreed; and**
- (ii) authority be delegated to the Executive Head of Transformation to amend the wording of paragraph 1.5, after consultation with members of the Committee by email.**

37/EC Records Management Policy

The Committee was informed that, although Records Management was briefly covered in the Information Security and Information Governance Strategy, adopting a specific Records Management Policy would provide a more robust management of records. Members considered a Records Management Policy which set out the standards for good records management to help ensure that the Council had the right information at the right time to make the right decision and help ensure it met its obligations under Data Protection legislation.

The Committee reviewed the Policy and recognised that it placed responsibilities on councillors to manage records in accordance with the Policy and related procedures. In view of this responsibility, it was recognised that councillors would need access to a secure area in which to securely store documentation, which was not currently available to them. The Committee therefore agreed to defer the adoption of the Policy in order to further look at options for Members to securely store documentation.

RESOLVED to defer agreement of the Records Management Policy pending the assessment of an option for Members to access a secure document storage solution.

38/EC Social Networking Policy

The Social Networking Policy aimed to provide guidelines for the effective and safe use of social networking to promote and develop the Council's services, and to ensure employees and workers were aware of how they should conduct themselves when using social networking sites both at work and outside of work.

The Social Networking Policy was regularly reviewed and the current review had recommended changes as set out at Annex A to the agenda report.

RESOLVED that the revised Social Networking Policy, as set out at Annex A to the agenda report, be agreed.

39/EC National Graduate Development Programme

The LGA's National Graduate Development Programme, which had been running since 2002, provided for local authorities to employ graduates on a two-year contract, where they undertook at least three different service placements. The LGA provided a complimentary training and development offer which included working towards an Institute of Leadership and Management Level 7 qualification. The LGA carried out the central multi-stage recruitment exercise and would refer successful applicants to local authorities to carry local interviews. It was noted that the creation of a graduate post would require a budget increase.

The Committee endorsed the proposal and suggested that it be extended with a view to recruit up to 3 graduate posts on a rolling programme.

RECOMMENDED to Full Council that

- (i) the Council creates three new posts of 'Graduate Trainee' and that it seeks to recruit to these roles via the Local Government Association's National Graduate Development Programme; and**
- (ii) the budget be increased accordingly.**

40/EC Extension of the Shared Monitoring Officer Role

The Committee was reminded that in October 2020, the Council had agreed appointment of Gavin Ramtohal as the shared Monitoring Officer with Elmbridge Borough Council. This had been on the basis that the initial agreement would be for a trial period of 6 months to provide both Councils with the opportunity to assess whether the arrangement was working and whether they wished to continue.

It was reported that the Monitoring Officer was satisfied that the agreement was working well and, as far as he was aware, Elmbridge BC was satisfied with the arrangement. The Committee was therefore asked to continue the contract as permitted by the existing contract on a rolling basis, meaning that the contract would continue from May 2021 until either Council decided to end the contract by giving the other at least one month's notice. It was recognised that any decision to continue with the shared Monitoring Officer was also subject to Elmbridge BC's agreement.

Members were updated on the recruitment to vacant positions within the Legal Services team and requested that the shared arrangement be reviewed again in 6 months' time, at which time further financial details concerning the arrangement with Elmbridge BC and the vacancies would be presented in an exempt report to the Committee.

RESOLVED that

- (i) the arrangements for sharing a Monitoring Officer with Elmbridge Borough Council continue on a rolling basis, with one month's notice for either party; and**

- (ii) a further report be brought to the Committee in 6 months' time containing financial details about the Monitoring Officer arrangement and the vacancies within the Legal Services team.

41/EC Urgent Action

The Committee noted Urgent Action undertaken in accordance with the Scheme of Delegation of Functions to Officers concerning the creation of the role of Head of Planning and disestablishing the role of Executive Head of Regulatory. It was advised that, as the decision was ultimately the responsibility of the Full Council, the Mayor and Leader of the Council had also authorised the Urgent Action taken.

RESOLVED to the urgent action taken under the Scheme of Delegation of Functions to Officers.

42/EC Appointment Sub Committee minutes

The minutes of the Appointments Sub Committee meetings held on 30 September 2020, 12 October 2020, 19 October 2020 and 17 February 2021 were agreed and would be signed by the Chairman of the Sub Committees at the next available opportunity.

43/EC Work Programme

The Committee considered a draft Work Programme for the 2021/22 municipal year. It was agreed to bring forward the Climate Change Policy item to the meeting in July 2021.

RESOLVED that the Work Programme for 2021/22, as set out at Annex A to the agenda report, as amended, be agreed.

44/EC Exclusion of Press and Public

In accordance with Section 100(A)(4) of the Local Government Act 1972 (as amended), the press and public were excluded from the meeting for the following items of business on the ground that they involved the likely disclosure of exempt information as defined in the paragraphs of Part 1 of Schedule 12A of the Act as set out below:

Minute	Paragraph(s)
45/EC	1
46/EC	1

Note: Minute 45/EC is a summary of matters considered in Part II of the agenda, the minutes of which it is considered should remain confidential at the present time.

45/EC HR Matter

The Committee received a report relating to an exempt matter.

46/EC Review of Exempt Items

The Committee reviewed the report which had been considered at the meeting following the exclusion of members of the press and public, as it involved the likely disclosure of exempt information.

RESOLVED that the information relating to minute 45/EC remains exempt.

Chairman

This page is intentionally left blank

Records Management Policy

Summary

The Records Management Policy was presented to the Employment Committee on 25th March 2021. It is being presented again to the Employment Committee with amendments to clarify that the Policy will be relevant for SHBC staff only and that members ICT practises be included within the Members Constitution.

Recommendation

The JSCG is advised to RESOLVE that the Employment Committee be asked to agree the Council's Records Management Policy, as set out at Annex A to this report.

1. Resource Implications

- 1.1 There are no additional revenue or capital cost implications arising from the report.

2. Key Issues

- 2.1 The Records Management Policy sets out the standards for good records management for all SHBC staff to help ensure that the council have the right information at the right time to make the right decision and help ensure it meets its obligations under Data Protection legislation.
- 2.2 Records Management is briefly covered in the Information Security and Information Governance Strategy, however by adopting a specific Records Management Policy that sits alongside these policies we aim to ensure a more robust management of records by giving SHBC staff more specific instructions on day to day management of records, ensuring records in whatever form they take are; accurate, reliable, ordered, complete, useful, up to date, are not kept for longer than necessary and are secure.

3. Options

- 3.1 The Group has the option to recommend the Records Management Policy to the Employment Committee, with or without any further amendments it considers appropriate.

4. Proposals

- 4.1 It is proposed that Records Management Policy is adopted.

5. Equalities Impact

5.1 Completed.

Annexes	Annex A – Records Management Policy
Background papers	None
Author/contact details	Sally Turnbull – Information Governance Manager Sally.Turnbull@surreyheath.gov.uk
Executive Head	Gavin Ramtohal, Executive Head of Legal Services



RECORDS MANAGEMENT POLICY

Document history

Date	Version	Author	Changes made
Feb 21	1.0	Sally Turnbull	Initial version

Approvals

Name	Signature	Role/Title	Date
Stuart Field		ICT Manager	Jan 21
James Rutter		ICT Manager	Jan 21
Gavin Ramtohal		Head of Legal Services and DPO	Jan 21
Sally Turnbull		Information Governance Manager	Jan 21
JSCG			

Document Filename and Location:

Filename: Surrey Heath Records Management Policy

Format	Version	Filepath	Owner
Draft	Draft 0.1		Sally Turnbull
Published			

Format	Version	Filepath	Owner

1. Introduction
2. Purpose
3. Objectives
4. Relevant Legislation
5. Relationship with existing policies
6. Key definitions
7. Roles and Responsibilities
8. Creation of Records
9. Storage
10. Retention and Disposal of Records
11. Classification
12. Business Continuity
13. Data Protection Principles of Information Management
14. Further Guidance and Review

1. INTRODUCTION

- 1.1 Information, in all its forms, whether electronic, paper-based or staff knowledge, is Surrey Heath Borough Councils (SHBC) second most important resource after our people. Records Management is at the heart of the way in which we deliver service to the public. If we do not have consistent and accurate records we cannot optimise our efficiency or measure the improvements; in order to achieve this, our records should be:
- (a) **Available** - Records will be available to those who need it, and who have the permissions to view or use it. We will avoid information overload and target information where it is needed.
 - (b) **Accessible** - Our records should be clearly identified and easily found when needed by anyone who needs to access it.
 - (c) **Electronic** - Our records and documents will be stored electronically. Over time, we will evolve our policies such that we will endeavour to only keep paper records where there is a legal requirement to do so.
 - (d) **Secure** - Records will be protected and retained as appropriate. We will record the confidentiality of information. Non confidential information will be openly published.
- 1.2 All records created and received by the Council, and its external service providers where they are processing information on the Council's behalf, are the property of the Council, and must not be used for any activity or purpose other than official Council business.

- 1.3 Failure to manage records properly within SHBC exposes the council to a significant financial, legal, confidentiality, public relations and potentially manpower-shortage risk.

2. PURPOSE

- 2.1 This policy sets out the Council-wide policy for records management standards that should be adhered to by all [SHBC](#) staff working with SHBC records including permanent and temporary employees including those who are agile working, working off-site and working jointly with partners, ~~elected members~~, volunteers, contractors, secondments and work experience placements.
- 2.2 The Records Management Policy is about how Surrey Heath receives, creates, communicates, stores, uses and distributes the information we need to deliver our services and corporate objectives.
- 2.3 This policy applies to all the Council's information and data sets in all formats - paper, electronic (including graphical, audio, photographic and video files) and, so far as feasible, staff knowledge, including those that the Council creates, holds on behalf of others or shares with third parties or partner organisations. All information, records and data sets including emails need to be stored in a manner that allows effective retrieval and allows the relevant retention rules to be applied.
- 2.4 The Policy will add value to the information resources used by the authority and will promote efficiency. It will show customers and citizens that the Council has a commitment to providing high quality information and takes its role as the custodian of information seriously.

3. OBJECTIVES

- 3.1 The objectives of the Records Management Policy are:
- (a) To instil an understanding of the importance, and an appreciation of the potential, of effective records management.
 - (b) To help develop awareness, understanding and to promote the application of good practice in handling information, and develop efficiency and effectiveness in this area.
 - (c) To support SHBC's ambition to improve processes, to improve customer services, to become more efficient and to reduce costs.
 - (d) To meet legislative and regulatory requirements and apply best practice.

4. RELEVANT LEGISLATION

- 4.1 Good records management must be managed in accordance with current legislation and existing professional standards. These include the following;
- Local Government Act 1972
 - Local Government (Access to Information) Act 1985
 - Data Protection Act 2018
 - Freedom of Information Act 2000
 - Environmental Information Regulation 2004
 - Re-use of Public Sector Information Regulations 2015
 - Public Records Act 1958 and 1967

- Human Rights Act 1998
- Lord Chancellors Code of Practise for Records Management
- In addition certain records will be subject to other legislation covering their subject area.

As well as key legislation there are useful guidance and procedures that should be consulted to ensure good records management these include;

- ICO guide to 'Records Management and Security'
- Cabinet Office 'Data Handling Procedures in Government'
- LGA 'Data and Transparency'

5. RELATIONSHIP WITH EXISTING POLICIES

5.1 This policy should be read in conjunction with the following related polices and guidance's;

- Information Security Policy
- Data Protection Policy
- Information Governance Strategy
- Email Guidance
- Corporate Style Guide
- Disciplinary Policy
- Offsite Working Policy

6. KEY DEFINITIONS

- 6.1 A "Record" is information held by the Council that relates to a specific topic, area of work or an individual. The record can be held in paper or electronic format
- 6.2 'Personal Data' is information that relates to an identified or identifiable person who could be identified, directly or indirectly based on the information.
- 6.3 "Records Management" is the planning, control, organisation and training activities relating to the creation, distribution, utilisation, storage, retrieval, maintenance, protection, preservation and final disposal of all types of records required for the conduct of the Council's activities
- 6.4 A "Records Retention Schedule" is a policy that defines how long records must be kept and provides disposal guidelines for how data items should be discarded. Records retention schedules are determined by the record type and the business, legal and compliance requirements associated with the data.

7. ROLES AND RESPONSIBILITIES

7.1 Corporate Management Team (CMT)

Are responsible for ensuring that the business areas they have responsibility for have processes and procedures in place that support this policy.

7.2 Data Protection Officer (DPO)

Is responsible for setting strategic direction and ensuring that policies and processes are in place for the safe management of information. The DPO is supported in this role by the Information Governance Manager.

7.3 **Information Asset Owner (IAO)**

Are responsible for ensuring appropriate information management practices including access controls and record retention and destruction are in place for their information assets (electronic and paper).

7.4 **Information Governance Manager**

Is responsible for working with the DPO to set strategic direction, ensuring that policies and processes are in place for the safe management of information.

7.5 **ICT**

Is responsible for providing and maintaining the secure infrastructure to enable information users to have access to information they require to deliver their services. In conjunction with Information Asset Owners and information users, the ICT Service will work towards the automation of the Council's archiving and records retention policy using cost effective and approved technology solutions.

7.6 **Line Managers**

Are responsible for ensuring their staff are aware of their information management responsibilities and arrangements for access to information, and that staff are appropriately trained or experienced.

7.7 **All staff**

All [SHBC](#) staff, ~~elected members~~, contractors, consultants and agents ("information users") are responsible for managing records in accordance with this policy and related procedures. When leaving the Council, all staff must ensure that key Council records for which they are responsible remain accessible.

8. CREATION OF RECORDS

8.1 Records should be created and captured in a timely manner. This should either be done by someone who has direct knowledge of the event or transaction, or generated automatically as part of a routine operation.

8.2 Where appropriate, when creating records current corporate templates should be used for all documentation both physical and electronic.

8.3 Website content should be produced in compliance with The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

8.4 Records should have meaningful titles and where applicable include indexes/metadata so that they can be retrieved quickly and efficiently

8.5 To reduce duplication which can lead to incorrect records being updated or available, records should be centralised with version control and dated.

8.6 Records should be complete and accurate enough to allow staff (including any successors) to undertake all actions for which they are responsible.

8.7 The creator of the record is responsible for ensuring that it is accurate, of good quality, relevant, up-to-date, and if includes personal, sensitive or confidential information it is secure.

8.8 ICT should ensure appropriate backup arrangements are in place for electronic records (including restoration of backups and disaster recovery if electronic records are damaged).

9. STORAGE

- 9.1 To maximise efficiency, reduce costs, enable appropriate access and sharing and minimise risks, records must always be stored securely in corporate repositories, these include:
- (a) **Filing cabinets**, physical storage accommodation for records should be clean and tidy, to prevent damage to the records, and securely protect against unauthorised access.
 - (b) **Microfiche or archiving system** (Alchemy) If applicable
 - (c) **The internet and intranet**. Both are extensive and contain a great deal of corporate information, including Committee reports and agendas (via the ModernGov platform), and a range of services and e-forms.
 - (d) **Microsoft Office and outlook**. All staff use the corporate systems, and calendars are generally open. Use of e-mail helps to share information but email should not be used as a storage of records instead records should be moved to the relevant service system or Box folder.
 - (e) **Box**. Each staff member has their own personal box folder, information of a confidential or sensitive nature should be stored within your own box folder and should be password protected. Only SHBC related data must be stored on Box. All services areas have their own box folder. Some of these are made available for corporate use either generally or on request while others are held and used locally within the service. The centralised filing structures in Box enable services to share documents and improve the security of our records. Box governance standards including access management, retention periods and classifications should be set when setting up box folders especially when the information being stored is of a personal or confidential nature.
 - (f) **Specialist Software Systems**. Specialist systems are used in some areas – these include; Northgate in Revenues and Benefits, Uniform in Planning, Licensing, Enforcement, Tree Protection, Listed Building and Land Charges, Civica in Finance, Xpress in Electoral Registrations and iKen in Legal. Access to these systems should be on a need to know basis and records should be managed in line with this policy.
 - (g) **Customer Relationship Management (CRM)**. The Plan Alpha CRM system holds documents and records of all customer contacts through Customer Services, together with additional information from some contacts through other services. Access to Plan Alpha should be on a need to know basis and records should be managed in line with this policy.
 - (h) **Geographical Information System (GIS)**. We have established a corporate platform for mapping information, with integration into a number of key databases, and browser-based delivery through the Xmap mapping services. Our Local Land and Property Gazetteer is the definitive source for addressing in the council and publishes nightly address change updates to the National Land and Property Gazetteer. Access to the GIS system is managed by ICT.
 - (i) **USB drives / memory sticks and other removable media**. In the majority of circumstances ICT will no longer supply removable media such as USB sticks to staff as they are no longer required. Additionally ICT monitoring systems will prevent their usage on SHBC supplied equipment. Removeable medias must not be used for permanent storage of records. If you are required to transfer records, on most occasions, you are advised to use the sharing tools within Box

which are secure and timely. Only removable media supplied by ICT Services should be used with SHBC systems, all removeable media supplied by ICT are encrypted to the correct standard.

- 9.2 Avoid storing duplicates (e.g. avoid paper/electronic overlaps, e.g. store a single copy of electronic information to be shared through use of box links) and routinely destroy unnecessary information (in accordance with the corporate retention schedule);
- 9.3 If the record being stored includes personal or sensitive data additional security measures must be taken to ensure that only staff that need to know have access to the data, this will include, setting access controls to specific staff, ensuring password are set to access the records and for physical records ensure they are securely locked away. Additionally, Box sharelinks can be set to expire a certain number of days after they have been created.

10. RECORDS RETENTION AND DISPOSAL

- 10.1 The retention and disposal schedule ~~that are~~is maintained by the IAO in each service area and centrally managed within the Information Governance Department, helps the Council to meet its statutory obligations to ensure that information is retained for the correct period of time and then disposed of appropriately. It is unlawful to retain information for longer than necessary.
- 10.2 Electronic information should be treated in the same way as physical information; therefore, electronic information, where the system allows, must be disposed of once it has reached its set disposal date.
- 10.3 Each department/section should have a records retention schedule/policy in place which will outline the appropriate retention periods for records. These retention periods should be based on legislative requirements and common practice in the sector. The retention periods listed in the schedule are the minimum length of time which the data, information and records must be kept. retention schedules should be regularly reviewed (at a minimum every three years).
- 10.4 Where systems have the functionality to set retention periods on records or groups of records, it is recommended that an intended disposal or review date is captured when creating the electronic records.
- 10.5 IAO will review records in accordance with the retention schedule, when they are no longer required for on-going business or specific legal or regulatory purposes, records will be securely destroyed.
- 10.6 At the end of the retention period, the record should be assessed to see whether it ought to be selected for permanent preservation, e.g. if it is of historical interest. Such records should either be retained by the Council or be offered to the Surrey History Centre for archiving
- 10.7 Records that could be subject to a Freedom of Information or Data Protection request must not destroyed unless the approved retention period has been met.

11. CLASSIFICATION

- 11.1 Where appropriate, the National Protective Marking Scheme classifications should be used. This provides for unclassified information and 3 levels of classification Official, Secret and Top Secret. In most cases local government information will fall into the lower category of UNCLASSIFIED. It is not necessary to mark each

document/email if it is official. If it contains sensitive/personal information you may wish to classify it Official – Sensitive in the subject field of the email.

12. BUSINESS CONTINUITY

- 12.1 Information Asset Owners are responsible for identifying the data, information and records (regardless of the media in which they are stored) which are considered to be business critical and to ensure that the business critical elements are included in individual service unit business continuity plans.
- 12.2 It is the responsibility of ICT to ensure that backups are created to the agreed standards and to establish an effective back-up restoration regime to ensure that when back-ups need to be restored they remain fit for purpose.

13. DATA PROTECTION, PRINCIPLES OF RECORDS MANAGEMENT

- 13.1 Information which is subject to security controls i.e. personal, sensitive, confidential data, will be identified, and will be held and used in accordance with a Data Protection regime appropriate to the nature of the information.
- 13.2 Public information will, so far as reasonably possible, be made available without charge.
- 13.3 Information will be retained, archived and disposed of according to a records retention schedules.
- 13.4 The Council has an Information Asset Register (IAR) that identifies the information assets owned by the Council. The IAR is subject to an annual review and any risks identified will be reported to the Information Governance Manager.
- 13.5 Email and c:\ drives will not be used to store council information, staff should only store case work and other council information in the location agreed by their IAO this will usually be a specific system used by that department or Service Area or another corporately agreed location within the Council network.
- 13.6 The IAO will ensure that where new systems that store personal data or any sharing of personal data with third parties is to be undertaken a Data Protection Impact Assessment is completed before the sharing can take place.
- 13.7 Where records are being shared or systems accessed by third party data processors, contracts with the appropriate Data Protection and records management clauses regarding the agreed and approved methods of information handling are included.

14. MONITORING AND REVIEW

- 14.1 This policy will be reviewed when required or at the minimum at least every 5 years. The Information Governance Manager will regularly monitor compliance with the policy procedures and guidelines making any amendments and improvements as necessary.

This page is intentionally left blank