INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Information Governance
TO:	Head of Governance and Monitoring Officer	**DATE:**	23 May 2024
C.C.	Chief Executive Head of Finance Portfolio Holder (Cllr Davison)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2023/24, an examination of the above subject area has recently been completed by Emma Walker, Internal Auditor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 The term Information Governance refers to how information is held, obtained, recorded, used, and shared by the Council. Information governance involves protecting confidentiality and ensuring that the right access levels are in place for both public and personal information.

2.2 Following the relocation of Council offices from Riverside House to Saltisford One, the Royal Pump Rooms, and the Town Hall, it was agreed that the scope of the audit would focus on how data security was maintained during the move.

2.3 As of a result of this, the content of the audit was largely driven by the data obtained through a staff survey which was used to identify how officers deal with data security in their new working environments. Some aspects of the audit were also discussed with staff from the relevant teams (e.g., the Corporate Support Team (CST)).

3 Objectives of the Audit and Coverage of Risks

3.1 The management controls in place have been assessed to provide assurance that the risks are being managed effectively. It should be noted that the risks stated in the report do not represent audit findings in themselves, but rather express the potential for a particular risk to occur. The findings detailed in each section following the stated risk confirm whether the risk is being controlled appropriately or whether there have been issues identified that need to be addressed.

3.2 In terms of scope, the audit covered the following risks:

1. Fines for non-compliance with legislation.
2. Breach of GDPR legislation, Data Protection Act 2018 and the Council's 'information governance framework'.
3. Reputational damage to the Council arising from data being inappropriately controlled.
4. Data obtained is used for fraudulent purposes.
5. Health and safety of vulnerable residents if data is not appropriately controlled.

3.3 A 'risk-based audit' approach has been adopted, whereby key risks have been identified during discussions between the Internal Auditor and key departmental staff. The Governance service area risk register and the Significant Business Risk Register have also been reviewed.

3.4 Whilst the work in this area does not have a direct impact on the objectives set out within the Corporate Strategy: Warwick District 2030, appropriate control of information underpins the general work of the Council in the achievement of these objectives. It is essential that the Council's information governance processes and procedures are robust, to ensure that information is effectively managed in line with laws, regulations, and documented policies.

4 Findings

4.1 Recommendations from Previous Reports

4.1.1 The current position in respect of the recommendations from the previous audit undertaken in March 2021 was also reviewed. The current position is as follows:

Recommendation	Management Response	Current Status
A guidance document, pulling together all issues identified, should be drawn up and distributed to all staff.	Agreed. A guidance document will be drawn up and issued accordingly.	A guide to data protection when agile working was drawn up by the previous Information Governance Manager and distributed to staff in May 2023.

Recommendation	Management Response	Current Status
A review of relevant contracts should be performed where contractor staff have access to Riverside House or other relevant Council properties to ensure that appropriate reference is made to data security.	Contract managers will be asked to review their contracts to ensure that the need for data security has been appropriately considered in each case.	Data security is considered during the early stages of procurement and subsequently written into legally binding contracts. Although less contractors have access to Saltisford, it needs to be made clear who is responsible for managing contractor access in the new offices. The Health & Safety and Premises Manager confirmed that there are two types of contractors: Warwickshire County Council contractors and Warwick District Council contractors (e.g. Pinners) who are expected to sign into the visitors' book. The Project Officer for the Office Relocation advised that a pre-start meeting was held with Pinners before works commenced, where an access agreement and health and safety arrangements for the duration of the works were discussed. This was the same process for the Warwickshire County Council contractors undertaking work on the showers at S1.
Management should take into account the health and wellbeing of staff in relation to current working conditions and the information governance implications of staff working in 'shared spaces' when taking decisions on future office needs.	These aspects will be given due consideration (in conjunction with relevant staff, such as HR and the Information Governance Manager) when future office needs are being considered.	Both staff health and wellbeing and working in shared spaces are covered in the agile working guidance issued to staff in May 2023.

Recommendation	Management Response	Current Status
A review of work-issued devices (such as mobile phones) should be performed to ensure that they are suitable for the work now being performed at home (or other 'off-site' locations).	ICT Steering Group will be asked to perform a review of devices currently in use and to identify the resourcing implications of providing replacement devices where necessary.	The Head of Customer and Digital Services advised that this was not taken to the ICT Steering Group as the group is not currently in operation; however, the ICT team did undertake a review of work-issued devices. As a result of this, all mobile devices issued to staff (phones/tablets) were either replaced or updated. These are now part of an InTune mobile device management platform which manages the apps that staff can install on the devices and ensures that they are kept up-to-date and secured properly according to a set policy.

4.2 **Financial Risks**

4.2.1 **Potential Risk: Fines for non-compliance with legislation.**

It is the aim of Warwick District Council (WDC) that all appropriate staff are fully informed of their obligations under the Data Protection Act 2018. If the Council were found guilty of breaching data protection legislation, it could face a fine of up to £17.5 million. It is, therefore, the duty of all officers to immediately report any actual or suspected information security breaches to their line manager. Disregard for the Council's data protection policies by employees may be regarded as misconduct to which the Council's dismissal and disciplinary procedures apply. It is also outlined in the Information Security Incident Management Policy that all WDC staff, contractors and third parties, should report details of any actual or suspected information security incidents.

Staff receive data breach training through Meta pop-ups, although these are currently being migrated to a cloud-based system; data protection training is mandatory for Members, and Councillors were last provided with information governance training in the summer of 2023 (there were three opportunities provided over June and July). From this, nine Councillors have not attended (although two of these were only elected in 2024).

Advisory – Consideration should be given to providing Members with Information Governance refresher training.

A survey was compiled by the auditor and distributed to all staff via the Intranet. The aim of this survey was to assess how data security had been maintained following the move from Riverside House (RSH) to Saltisford One (S1), The Royal Pump Rooms and the Town Hall. It was agreed with the Head of Governance that the survey would be of a similar nature to the last information governance survey conducted as part of the audit in March 2021. The April 2024 survey received 118 responses in total. 82% of the staff who responded to the survey said that they had received appropriate training on how to report a data breach. Examples of incident levels and possible responses to data breaches are outlined in the Information Security Incident Management Policy, which is available to all staff through the Intranet. This policy is, however, in need of an update, as it still refers to the post of Democratic Services Manager and the ICT Steering Group, which is not currently in operation.

Recommendation – The Information Security Incident Management Policy should be reviewed and updated, as appropriate.

Incidents involving potential or actual data loss are rated on a scale of 1-5. Incidents rated at levels 3-5 are classed as major security incidents. A major incident is defined as a loss, potential loss, or breach of confidentiality of any information owned by WDC that is classified at the confidential or restricted levels. The Information Security Incident Management Policy outlines the steps to be taken when reporting an incident, including the various facts to be established:

- What happened?
- When did it occur?
- Who was involved?
- What information assets were compromised/lost/disclosed/put at risk?
- What security measures were in place?
- What is the impact on the individuals' privacy?
- What is the impact on WDC, or other services?
- What immediate actions have been taken to minimise risk, recover any data loss and inform individuals/organisations affected?

Information Governance training for all staff is mandatory through the meta-eLearning portal as part of staff inductions; staff are also required to periodically complete refresher training.

Advisory - Following reports of data breaches at other local authorities, consideration should be given to rolling out information governance refresher training to all staff.

At present, the Information Governance Manager (IGM) role shared with Stratford-on-Avon District Council (SDC) is vacant. The service is looking to recruit for a permanent role and a report to this effect was sent to Cabinet on 10 April 2024. Since the summer of 2023 there have been new Heads of Service for this arrangement at both SDC and WDC and it was agreed to explore the option of increasing the team to make it more robust (recognising the demands at both Councils). Two of the four posts have been advertised and one of the four posts is now occupied. In addition to this, the SLA is now being drafted to ensure that arrangements are in place for the service to start as soon as possible. As an

interim measure, WDC information governance queries are passed to the Head of Governance.

The WDC Data Protection and Privacy Policy outlines the roles and responsibilities of various individuals. The Chief Executive and Deputy Chief Executive are responsible for ensuring a co-ordinated response from the Council and for keeping under review the Council's approach to personal information, data protection and privacy. Heads of Service are responsible for the information assets under their control, including personal information. They are responsible for making sure that employees who access or handle personal information are suitably trained in data protection and privacy. Heads of Service are accountable, as Information Asset Owners, for ensuring that all information risks relating to their information assets or service areas, are properly assessed and action is taken where necessary to reduce the Council's information risk exposure.

To test this, a number of risk registers were reviewed by the auditor to ensure that Heads of Service had appropriately incorporated data protection measures into their risk management arrangements. Of the six 2023/24 service area plans published, only two (Finance and Governance) had 'failure to comply with GDPR/data protection' as a named risk.

Advisory – Consideration should be given to asking Heads of Service to include data protection risks/the risk of data loss within all service risk registers.

The Data Protection and Privacy Policy makes clear that every employee is responsible for the appropriate use and protection of personal information which is in their possession or use. A signature of receipt and understanding of this policy, as well as the WDC Code of Conduct, is included in new starter employment packs.

The Information Security and Conduct Policy outlines the responsibilities of the Employment Committee, HR, Heads of Service, line managers, system owners, ICT services, Internal Audit, and the IGM. All end users of information systems are responsible for ensuring that the Information Security and Conduct Policy is complied with.

4.3 Legal and Regulatory Risks

4.3.1 Potential Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.

There is a Data Protection and Privacy Policy in place, accessible to all staff through the Intranet. The policy sets out the Council's requirements regarding the appropriate and responsible use of personal and private information.

Under this policy, personal information can be shared with other organisations (such as contractors or government bodies) in the interests of the individuals concerned, or for purposes deemed to be in the public interest. The policy has, however, not been updated since 2018 and should be reviewed every twelve months by the Data Protection Officer.

Recommendation – The Data Protection and Privacy Policy should be reviewed and updated, where appropriate.

The Council has other policies, sub-policies, and guidance in place on the use of personal information, which form part of the Council's Information Governance Framework. The General Data Protection Regulation (GDPR) requires the Council to keep a record of all personal datasets that it holds with essential details about collection (legal basis), use, security, sharing, and retention. The Head of Governance maintains a spreadsheet which tracks the progress of all Council data privacy impact assessments (DPIAs). This was last updated in April 2024 and outlines the status of the necessary agreements/projects in place where the processing of data must be appropriately managed; this includes a description of the assessments and the relevant lead officers.

There is also a DPIA toolkit in place which serves as a guide for project managers to support them when completing and reviewing DPIAs. The DPIA template assists in the initial assessment of impact on personal information when considering service or system changes. The toolkit also ensures that data owners evaluate the reasons for holding certain data.

Staff are tested on Meta Compliance to ensure that they have read and understood the Data Protection Policy. The latest meta pop-up on sharing information with third parties was released on 31 August 2023. As part of the Information Security and Conduct Policy, all users must receive appropriate information security awareness training. There have been numerous meta compliance pop-ups on data handling, information security, the Information Governance Framework and privacy notices.

Under useful links on the Intranet, staff can check their compliance portal to view any mandatory policy training that they must complete; staff receive e-learning reminders for ten weeks if they have not completed the necessary training. The system also leaves an audit trail which signals when data protection training was last completed by officers. Although staff have been issued with guidance and meta reminders regarding data protection when working from home, the Learning & Development Officer is working with the Office Relocation Project Manager to roll out new working environment Meta-training to all staff.

Advisory – Consideration should be given to compiling refresher training (meta pop-ups) on password security and suspicious email links.

The Council's Information Security and Conduct Policy provides guidance on the arrangements that must be in place to ensure that personal data is kept protected and secure; however, this policy has not been reviewed since 2020.

Recommendation – The Information Security and Conduct Policy should be reviewed and updated, as appropriate.

The information security responsibilities of users must be defined and incorporated into the induction process and contracts of employment; the Learning & Development Officer advised that these responsibilities are not

specifically written into employment contracts, but they are included in the WDC terms and conditions which all new starters must sign. Encouragingly, 104 of the 118 survey respondents said that they had read the Council's Data Protection Policy. Despite this, 80 respondents felt that they had not been made aware of any data policies or procedures following the move to the new offices, where previously this was only 62 in March 2021.

Recommendation – Following the office relocation, data policies and procedures should be updated to reflect new working environments, and these should be disseminated to all staff.

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under GDPR legislation to maintain the confidentiality of personal data. As a result of this, one of the questions posed to staff in the survey, was centred on the risks around forwarding work-related emails to personal email addresses and vice versa. Although 70% of the staff surveyed said that they did not forward work emails to personal email addresses, 30% of respondents continued to do so.

The main reasons provided for this related to payslips, BUPA receipts, site inspection photographs and any articles of interest. According to the Council's Email Acceptable Usage Policy, staff who use the Council's email systems for personal email are encouraged to store personal emails in a clearly identifiable mailbox folder. Personal emails that are not stored in a clearly marked folder are liable to be treated as business communications. It is up to the employee to prevent the inadvertent disclosure of the content of personal emails by filing personal emails in accordance with this policy.

Recommendation – Guidance needs to be disseminated to staff reiterating the Email Acceptable Usage Policy and highlight that the forwarding of work emails to personal email addresses, or vice versa, is strongly discouraged.

There was no formal communication regarding data security following the move to the new offices; only that staff were encouraged to take the necessary data with them.

There are seven key principles to which data must adhere in order to be classed as compliant with GDPR. 83% of staff surveyed said that they were aware of these seven key principles.

- Lawfulness, fairness, and transparency – there must be a lawful reason to collect the data.
- Purpose limitations – data subjects should understand the reason for providing personal information and have reasonable expectations about what the organisation will do with it.
- Data minimisation – only collecting the minimum data needed to meet the purpose of the organisation.
- Accuracy – data collected must be accurate; information should be updated on a regular basis.
- Storage limitation – data can only be kept for the duration defined within the original requirements.

- Integrity and confidentiality – data should be securely processed to avoid data breaches. Data can only be accessed and managed by those who have appropriate authorisation and should be recoverable.
- Accountability – those processing personal data should take responsibility to adhere to these principles.

The WDC Data Protection and Privacy Policy refers to the principles of GDPR, although this refers to only six principles of GDPR where there are now seven. The Appropriate Policy document regarding special category and criminal offence data also refers to the key principles of GDPR.

During the staff survey, questions were asked regarding the anonymisation of data. Each data set is reviewed on a case-by-case basis before it is released; actual data content and how this will be used determines whether it is anonymised prior to its release. The survey revealed that most officers are not required to anonymise data as part of their role (80%). Of the twenty-three respondents that are required to anonymise data, only six have access to a redaction tool. Whilst some officers said that redacting is conducted by the CST or documents are password protected, other officers advised they would appreciate access to a tool of this nature.

Advisory – Consideration should be given to extending the redaction tool software license.

4.4 Reputational Risks

4.4.1 Potential Risk: Reputational damage to the Council arising from data being inappropriately controlled.

A section of the survey focused on questions around staff working spaces and devices. In the home, equipment should be located out of sight of the casual visitor and other family members. For home working it is recommended that the office area of the house should be kept separate from the rest of the home. The majority of respondents surveyed (49) described their working space as a separate home office or study. This shows a positive improvement from the last time the survey was conducted, in which the majority of respondents (57) described their working space as a desk in a communal room of the house.

99 out of 118 respondents stated that their working space is not used by other people; this pattern has remained fairly static since the time of the last survey in which 108 of 161 respondents said that the space was not used by others. Reassuringly, 48% of those surveyed said that they also wear a headset when on call at home and 88% of staff continue to wear a headset in the office. It was found that most officers (53) work from home five days a week; highlighting the necessity to ensure that data security is watertight.

Although most of the people surveyed said that they did not have any listening devices in their home (81), of those that responded 'yes' to this question (37), the majority said that they did not turn these devices off when working (21). This has seen a decline from the previous survey where 133 respondents said that they did not have listening devices in their home.

Recommendation – Guidance should be issued to staff around listening devices and the risks that these introduce to data protection when working from home.

101 of the 118 respondents said that they felt they had received appropriate training on data security when working from home; this was a similar result to the last survey where 107 of 161 respondents also felt that they had received appropriate data security training. Some respondents (14) requested specific data training in the survey, with topics including listening devices in the workspace, data breaches, disposal of notepads, printing at home, general tips/awareness, and refresher guidance, including a potential Intranet page dedicated to data protection when working from home. These topics were of a similar nature when compared to the results of the 2021 survey.

Advisory – Consideration should be given to compiling training based on the topics requested by officers.

When accessing Council systems or data outside of Council-controlled environments, computer terminals should be positioned to reduce the risk of being overlooked during use. It is essential that access to all confidential or restricted information is controlled. This can be done through physical controls, such as locking the home office, or this can be done logically by password controls. 90% of staff who responded to the survey said that they lock their screen when working from home; 95% of respondents said that their screens are positioned to ensure that they are not visible. This has increased since the last survey where only 88% of respondents said that their screens were not visible.

92 of the 118 respondents stated that they do not use personal equipment for work. Of the officers that responded 'yes' to this question (26), the majority stated that they use a personal home printer (7). The Agile Working Policy states that WDC printing is not permitted on home equipment.

Recommendation – Guidance should be disseminated to both staff and Members reiterating that printing from home is not permitted.

Advisory – Consideration should be given to conducting a 'deep-dive' into home-printing in order to understand the reasons why officers choose (or consider the need) to print from home.

Other respondents said that they used tablets for team meetings and personal laptops or mobiles. It is worth noting that staff also commented on the fact that they have to hold Zoom meetings on personal devices, as WDC do not support the Zoom license. The decision not to permit the use of Zoom was taken at a time when Zoom was a formative product with recognised and well publicised information governance risks.

Advisory – Consideration should be given to permitting the use of Zoom on WDC equipment connected to the network.

Twenty-four respondents stated that they collect printing or post from the CST or directly from the offices. This figure has seen only a slight decline since 2021 wherein thirty-four respondents collected printing/post through these methods.

The Data Handling Policy details the basic requirements and responsibilities for the proper management of information assets at WDC. The policy specifies the means of information handling, transfer, and disposal within the Council and applies to all systems, people, business processes and documents that make up the Council's information systems. This policy, has not, however, been updated since 2014, and refers to roles and working groups that no longer exist; it is also stated in the policy that it should be reviewed every twelve months.

Recommendation – The Data Handling Policy should be reviewed and updated, as appropriate.

Internal information is generally available to all staff on a need-to-know basis, as decided by their line manager. Confidential and restricted information is available only to staff who have a business need to know the information, and with the approval of the relevant system or Information Asset Owner. The transfer and exchange of information concerning identifiable living persons is subject to the Council's Data Protection Policy. The Information Commissioner's Office has stated that organisations are responsible for information that is held not only on equipment owned by them, but on personal equipment that they know is being used by their employees.

A remote-working policy is in place to ensure that staff are aware of their individual responsibilities around information security when working remotely. The policy also provides guidance for staff on secure remote working to minimise the risk of unauthorised access to, or loss, of data. It should be noted that the Remote Working Policy still refers to the Home-Working Policy which has since been replaced by the Agile Working Policy.

Recommendation – The Remote Working policy should be updated to reflect the new Agile Working Policy.

In the event that Council owned equipment or information becomes lost or stolen, users must report the loss/theft to their line manager who will notify the ICT Services Helpdesk. If privately owned ICT equipment is used to produce Council related documents, or is used to access systems such as e-mail, then the employee or Member is responsible for ensuring all such documents and any downloaded data is stored securely or deleted.

As laid out in the Data Handling Policy, all information must be stored and handled (including transferred and exchanged) appropriate to the WDC Information Handling, Storage and Disposal Standard. Where appropriate, special storage equipment and environments should be used. Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units, and by ensuring that files and computer monitors are not left open to general or casual view.

The staff survey revealed that the majority of officers store data on their password protected WDC laptops (55%). Encouragingly, an increased number of

officers (15%) said that they do not keep any physical data at home; during the previous survey, only 4% of respondents provided this answer. Data is also being stored less in boxes and bags (9%) and more in secured drawers, cupboards, or locked home offices (20%). 87 respondents stated that they do not store physical documents at S1 or the Town Hall; given such a high number of responses to this question, it is possible that officers remain unsure as to the whereabouts of team documentation following the move.

Recommendation – Managers should be reminded to inform their teams where data is stored and located.

Of the thirty-one respondents who answered 'yes' to storing documents in the office, the majority of these said that documents are kept in locked cupboards (13): other answers included filing cabinets/drawers (4), access coded rooms (3) and storage rooms (5).

The deed store previously located at RSH has been moved to the Town Hall, although some files such as leases and building surveyor information is held at S1. There is an inventory of what is held in the deed store which is maintained by the CST.

If the decision to dispose of a document is taken, then consideration should be given to the method of disposal to be used. Minimum retention periods for certain financial information are stipulated by the VAT Act 1994 and the Taxes Management Act 1970. In order to calculate the right retention period for personal data, the following matters are considered:

- The amount, nature, and sensitivity of the personal data.
- The potential risk of harm from unauthorised use or disclosure of personal data.
- Any legal or regulatory requirements.

As part of the new information governance project, a formal data retention schedule will be compiled detailing the timescales in which data must be disposed. This will include the disposal of data retained digitally on individual staff H drives. The Head of Customer and Digital Services is looking to automate server migration to SharePoint to help avoid unnecessary data retention.

Advisory – Consideration should be given to promoting the active cleansing of staff personal drives.

Performance monitoring is in place regarding data quality and the management of data protection activities. As part of the Governance Service Area Plan, KPIs include:

- the % of Subject Access Requests (SARs) responded to on time (within ten working days). The target is 100% with progress currently at 82%. This KPI is monitored monthly through the WDC SAR database.
- the % of Freedom of Information (FOI) requests responded to on time (within ten working days). The target is 90% with progress currently at 92%. This KPI is monitored monthly through the FOI database.

4.5 Fraud Risks

4.5.1 Potential Risk: Data obtained is used for fraudulent purposes.

WDC may periodically receive requests from customers or suppliers to provide confidential, sensitive, or personal information. To determine the need for a contractual, binding agreement between parties, an appropriate risk assessment must be undertaken. There are several information sharing arrangements in place across the Council and part of the early procurement stages involves looking at data handling and confidentiality being written into procured contracts.

The staff survey revealed a fairly even split between officers who do (45%) and do not (54%) share sensitive data with external bodies. Of the officers that do share information externally, most respondents said that they do this via emails with partner agencies such as Warwickshire Police or Trading Standards (14). Some respondents also commented that information sharing agreements are in place, whereby information is not shared unless a confidentiality statement or consent to share has been signed by all parties involved (12).

For the purpose of shared projects with SDC, both Councils are joint data controllers. Each of these projects has its own data-sharing agreement and DPIA which sets out the personal data that will be shared. The appropriate Head of Service is responsible for ensuring that the Data Owner is meeting their responsibilities with relation to data protection. The IGM, as Data Protection Officer, is responsible for reviewing all data-sharing agreements and project DPIAs before they can be approved.

All significant information and record systems should be recorded on the Council's Information Asset Register. The Head of Governance advised that this is not currently up to date. A new bill is due to go through Parliament to change the ROPA (Records of Processing Activities) requirements. As a result of this, the Head of Governance is waiting to hear on the outcome of the Bill so that it can be built into WDC data record systems. The latest government guidance suggests this will be a phased implementation over two years.

The possible need to maintain evidential integrity should be considered when this record system is created. All information must be disposed of or sent to archive, in accordance with the Council's corporate retention and disposal schedule. Records may only be disposed of in a secure and controlled way that ensures destruction and provides a full information trail. Some records may be considered of future historical interest and the County Records Manager should be consulted regarding their possible preservation.

Disposal of documents other than those containing confidential or restricted information may be disposed of by binning, recycling, deletion (in the case of electronic documents), or the transfer of documents to external bodies. Records of disposal should be maintained by each service area, and the transfer, long-term retention or disposal of such documents must be authorised by the relevant Head of Service. The Head of Governance advised that once the new data retention schedules are in place, there will be no need for managers to

keep such detailed records of data disposal; however, staff will be asked to evidence that they have disposed of data each year.

The new home working DSE (Display-Screen Equipment) assessments ask staff various questions regarding data security including:

- Is access to your work on a computer password protected and is the password secure?
- Is your work secure from interference/observation from other members of the household?
- Is your workstation set apart from where you socialise?

Due to the fact that S1 is shared with upstairs tenants and given the recent issues concerning threatening behaviour from a member of the public, staff have been reminded not to allow individuals to tailgate them into the office; staff should ensure security doors (those fitted with card readers) are closed behind them. It is also outlined in the Physical Environment Security Policy that all staff must use their own ID card to access controlled areas of the building. It should be noted, however, that the Physical Environment Security Policy, only refers to RSH.

Recommendation – The Physical Environment Security Policy should be updated to reflect the move to the new offices.

Excluding weekends, bank holidays and public holidays, Warwickshire County Council (WCC) caretakers open S1 at 6.30am and close it at 6.30pm; the car park is closed at 7pm. WCC are responsible for cleaning the building; however, WDC remain responsible for the confidential waste contract. Cleaning requirements are included in the building lease and as part of the service charges paid by WDC, WCC will clean the windows, empty refuse bins, clean signage, clean the lifts, clean the floors, and clean the toilets and equipment in the common parts of the building. It should be noted that there is nothing specific in the agreement with WCC regarding data potentially being seen at S1 by WCC contractors/cleaners.

There is no delivery area on site at S1 and, therefore, deliveries should be made to the appropriate site and not to S1 by default. If there is no alternative other than to use S1 as the delivery address, the name of the officer ordering the item should be used on the delivery label and officer contact details (including phone numbers) should be given to the supplier. Officers are responsible for their own deliveries and should make sure that they are on site to receive their items. Deliveries should also be stored away, and any packaging disposed of appropriately.

Advisory – Consideration should be given to reminding staff not to have deliveries sent to S1 if they will not be present to accept them.

The printers at S1 are sited appropriately to avoid compromising confidential information. At the Town Hall, a printer is located in the WDC working area which requires a pass to access it, the other printer is in the back office to the reception area; however, this will be reevaluated once building works

commence. There is also a printer and a separate scanner located behind the reception in the Pump Rooms.

As part of the Physical Environment Security Policy, doors and windows should be locked when unattended and external protection should be considered for windows at ground level. S1 is open plan and officers are visible from the ground floor. Through observation conducted by the auditor during early morning hours, it was found that blinds had been left open, meaning that there is a risk of equipment being left visible to the general public.

Recommendation – Staff working at S1 should be reminded to close blinds at the end of the working day.

It is under the remit of WCC as the landlord, to regularly test the intruder detection system, covering all external doors and accessible windows at S1, although there is nothing specific in the lease about intruder alarm testing. The Facilities Manager for WCC did, however, confirm that the automatic doors at the front of the building are serviced as part of the routine maintenance programme. The caretaker also undertakes a check on the fire doors to ensure that they open freely and without issue. It is, however, the responsibility of all building users to report any issues with the building to the Facilities Hotline.

The Head of Governance confirmed that WDC are able to alarm the ground floor whilst ensuring that the upstairs tenant can still vacate the building without triggering the alarm. The Services Officer advised that WDC contractors are given passes allowing them limited access through the initial door set at S1 and then into the small foyer where they can access the key safe for other properties. This does not allow contractors access into the offices themselves and does not apply to WCC contractors who the Senior Building Surveyor Project Manager advised have contractual rights to enter WDC areas.

A guide to data protection when homeworking was compiled by the previous IGM and distributed to staff in May 2023. This guidance includes working in private rooms with few distractions, away from family members and in a location where conversations will not be carried. The guide also contains images of how to check email recipients and attached files before sending.

In terms of data disposal, the vast majority of staff surveyed said that data is either shredded at home (26) or disposed of via the confidential waste bins at S1 (29). 30% of respondents said that they did not keep confidential data at home, whilst 14% of respondents said that they either electronically deleted data from their recycle bin or burned/composted physical paperwork. These figures present a fairly similar pattern to those gleaned from the 2021 survey wherein:

- 34% of respondents said that they did not hold confidential data at home.
- 22% of respondents shredded paperwork at home and
- 16% of respondents electronically deleted data.

The latest survey revealed that more staff now make use of the confidential waste bins in the office, compared to those surveyed in 2021 (17).

It is the responsibility of the Information Asset Owner to ensure the secure disposal of information when it is no longer required. All items of equipment containing storage media (e.g. fixed hard disks) must be checked by ICT Services to ensure that any sensitive data and licensed software is removed or overwritten prior to disposal. Destruction of confidential or restricted WDC information captured on electronic storage media must only be performed with methods and equipment approved by ICT Services.

Heads of Service are responsible for determining whether to retain or dispose of specific documents within the remit of their service area. Staff were encouraged to only take the necessary data with them during the move from RSH to S1; this was championed by the Project Relocation team. The Head of Governance advised that extra secure containers had to be provided by Shred-It Ltd in order to cope with the extra confidential waste; however, much of the data transferred to S1 was digital in nature, with the majority of paper storage moved to the Town Hall over three secure rooms.

Staff have been given specific guidance in relation to information governance whilst working from home; this was last updated in March 2023. Laptops, removable devices and WDC mobile phones should always be locked when unattended. If working from home or another location, the working environment must be suitable and free of interruptions with due regard to confidentiality. WDC retains the right to withdraw agile working arrangements if data confidentiality is not maintained.

All employees should abide by WDC's Data Protection Policies and Procedures. It is the employee's responsibility to ensure that all data is always kept secure. There is an implied duty not to disclose confidential information or use it for any purpose other than WDC's business.

4.6 Health and Safety Risks

4.6.1 Potential Risk: Health and safety of vulnerable residents if data is not appropriately controlled.

In terms of the current post handling and distribution process, this is the biggest risk that the CST face. The Corporate Support Assistant advised that incoming post is dealt with as it was at RSH. Once the post arrives, it is sorted into pigeonholes in the post room. The post is then opened and scanned to the L drive post folder; the paperwork is retained for one month in a locked post room. There is a scanner in the hot desk area at the Town Hall, so some mail is taken for scanning and returned to the post room when complete.

For outbound mail, the mail items are gathered, recorded, and boxed up in the post room. The mail trolley is placed by the front door of the Town Hall for Royal Mail to collect around 4pm. The biggest risk for outbound mail is the fact that it is placed in an open area at the Town Hall; however, it needs to be in an obvious space for Royal Mail to find. The trolley is visible to Town Hall reception staff and this process will be improved by the introduction of hybrid mail.

Staff have been advised to no longer use the RSH postal address; instead, the Town Hall address should be on all letterheads. These letter templates are

downloadable from the Intranet or accessible on the L drive. Staff have also been advised to inform contacts that letters should be sent to the Town Hall as the official WDC contact address; email signatures have been updated to reflect this.

A review of the Intranet letter templates was conducted by the auditor. It was found in twenty-two cases, that the WDC contact address and job roles or departments were all correct. Four letters were generic in nature and therefore did not contain the relevant addresses or role titles. There was just one letter where the template referred to the wrong job title; however, this has since been passed to the CST for correction.

CST staff have been given data protection training and are aware of their roles and responsibilities when handling data. There have, in the past, been issues where multiple inserts relating to two different residents have been sent to one recipient; however, this has not occurred for some time. As highlighted in the Cabinet report, a fully functional Information Governance team will help better accommodate the new ways of working for the CST at the Town Hall.

As of September 2023, two new print queues were rolled out to staff. The Home queue has a longer hold time for documents which can be held on the server for up to 72 hours. After this time, any document not released for printing is deleted; the hold time on the WDC Standard printer is 24 hours.

Confidential waste bins were previously in situ at RSH; these are now in place at S1 and at the new Pump Rooms reception. Whilst there has been no active promotion of the confidential waste bins, auditor observation has confirmed that staff frequently use them. The Head of Governance confirmed that there are four bins at the Town Hall, with one of these having been placed behind reception. It is essential that any documents which are to be thrown away and contain confidential or personal data must be disposed of in this way, in order to avoid breaches of confidence or breaches of the Data Protection Act 2018.

A confidential waste contract has been in place since 1 August 2022; this is not due to expire until the 3 November 2025. There is, however, only £205.38 left to spend against this contract as expenditure has amounted to £9,194.62 thus far. It was found through a preliminary review of the purchase orders, that expenditure had included confidential waste removal at the Town Hall and S1. The Neighbourhood Services Manager is aware that the spend has increased significantly, due to new sites being added to the contract as well as the clear out of RSH. The Contract Operations & Performance Manager and Neighbourhood Services Manager are in communication with the Procurement team to make the contract compliant.

The Physical Environment Security Policy reiterates that all confidential information and removable storage media should be removed from desk surfaces when not in use, particularly prior to employees' departure from Council premises each evening; the clear-desk policy is included in the S1 standard operating procedure. It is also a requirement of the operating procedure to close the blinds, wear a headset when on call, and not disclose confidential information due to the open plan nature of the office. Staff are also reminded to lock computers when away from desks. The Town Hall operating

booklet was reviewed by the auditor; it was found that the clear desk-policy and use of headsets had not been replicated in this document.

Recommendation – The Town Hall operating procedure should be updated to reflect the clear-desk policy and use of headsets in the office.

97 of the 118 staff surveyed said that they had been made aware of the clear-desk policy following the move to S1. Despite this, auditor observation found that a large portion of desks had belongings left on them, and in some cases, work laptops. Storage cupboards were also left open with folders exposed; this mainly occurs around the Building Control, IT and Assets areas which poses a greater risk where blinds have been left open. The audit identified that, at present, there is no guidance in place about the steps officers should take when they see belongings or laptops left on desks at the end of the working day.

Recommendation – Staff should be reminded of the clear-desk policy. If staff are working at S1 on a continuous basis, laptops need to either be taken home or kept in a securely locked location. Staff also need to be made aware of who to report issues to or the actions to take if belongings are identified on desks.

WDC attempt to reply to SARs as quickly as possible, within the forty days allowed by the Data Protection Act 2018. Members of the public have the right to request access to certain information that the Council holds. Such requests may be:

- SARs (requests for personal data) made by the individual, or on behalf of the person who is the subject. These requests are dealt with under UK GDPR and the Data Protection Act 2018; or
- FOIs (requests for other information including personal data relating to a third party) made by anyone. These requests are primarily dealt with under the Freedom of Information Act 2000 (FOIA).

The FOIA covers any recorded information, and this can include printed documents, computer files, letters, e-mails, photographs, sounds, and video recordings. The Council can also refuse to provide information under the FOIA if the request would take over eighteen hours to deal with. A SAR may be made verbally or in writing and can be directed to any officer of the Council; it may be made via social media at any time to any person.

Data subjects have the right to know how long their personal data will be retained for future processing and have to opt-in for electronic marketing communications. WDC ensures that all individuals providing information about themselves, or other people, are aware of the way in which that information is held, used, and disclosed. A list of all service privacy notices is on the WDC website, highlighting to users how their data is stored, handled, and used. It should, however, be noted that the previous Data Protection Officer details are still on the website.

Recommendation – The Data Protection Officer contact details should either be removed or updated.

5 Summary and Conclusions

5.1 Section 3.2 sets out the risks that were reviewed as part of this audit. The review highlighted weaknesses against all of the identified risks.

5.2 Further 'issues' were also identified where advisory notes have been reported. In these instances, no formal recommendations are thought to be warranted as there are no significant risks attached to the actions not being taken.

5.3 In overall terms, we can give a MODERATE degree of assurance that the systems and controls in place in respect of Information Governance are appropriate and are working effectively to help mitigate and control the identified risks.

5.4 The assurance bands are shown below:

Level of Assurance	Definition
Substantial	There is a sound system of control in place and compliance with the key controls.
Moderate	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management.

6.2 The advisory comments above are reproduced in the attached Action Plan (Appendix B) for management consideration.

Ian Davy
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Information Governance– May 2024

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.1	Financial Risk: Fines for non-compliance with legislation.	The Information Security Incident Management Policy should be reviewed and updated, as appropriate.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025
4.3.1 (a)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	The Data Protection and Privacy Policy should be reviewed and updated, where appropriate.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.1 (b)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	The Information Security and Conduct Policy should be reviewed and updated, as appropriate.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025
4.3.1 (c)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	Following the office relocation, data policies and procedures should be updated to reflect new working environments, and these should be disseminated to all staff.	Medium	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.1 (d)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	Guidance needs to be disseminated to staff reiterating the Email Acceptable Usage Policy and highlight that the forwarding of work emails to personal email addresses, or vice versa, is strongly discouraged.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025
4.4.1 (a)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Guidance should be issued to staff around listening devices and the risks that these introduce to data protection when working from home.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.1 (b)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Guidance should be disseminated to both staff and Members reiterating that printing from home is not permitted.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025
4.4.1 (c)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	The Data Handling Policy should be reviewed and updated, as appropriate.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.1 (d)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	The Remote Working policy should be updated to reflect the new Agile Working Policy.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025
4.4.1 (e)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Managers should be reminded to inform their teams where data is stored and located.	Low	Head of Governance	Request to all managers via email can be sent for them to brief and explain to their teams.	31 July 2024
4.5.1 (a)	Fraud Risk: Data obtained is used for fraudulent purposes.	The Physical Environment Security Policy should be updated to reflect the move to the new offices.	Low	Information Governance Manager	This is accepted and the plan for the new Information Governance Team is to review and update all polices across both Council's. This review will be undertaken once the new IG Manager is in post and has evaluated the current position of each Council alongside the requirements of the implementation of the Data Protection and Digital Information Bill.	31 March 2025

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.1 (b)	Fraud Risk: Data obtained is used for fraudulent purposes.	Staff working at S1 should be reminded to close blinds at the end of the working day.	Medium	Facilities Manager	This will be included in the 'five things you need to know' email distributed to all staff.	7 June 2024
4.6.1 (a)	Health & Safety Risk: Health and safety of vulnerable residents if data is not appropriately controlled.	The Town Hall operating procedure should be updated to reflect the clear-desk policy and use of headsets in the office.	Low	Facilities Manager	The Head of Assets to liaise with the Facilities Manager on this.	31 July 2024
4.6.1 (b)	Health & Safety Risk: Health and safety of vulnerable residents if data is not appropriately controlled.	Staff should be reminded of the clear-desk policy. If staff are working at S1 on a continuous basis, laptops need to either be taken home or kept in a securely locked location. Staff also need to be made aware of who to report issues to or the actions to take if belongings are identified on desks.	Medium	Facilities Manager	This will be included in the 'five things you need to know' email distributed to all staff.	7 June 2024
4.6.1 (c)	Health & Safety Risk: Health and safety of vulnerable residents if data is not appropriately controlled.	The Data Protection Officer contact details should either be removed or updated.	Medium	Head of Governance	Agreed.	7 June 2024

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High: Issue of significant importance requiring urgent attention.
Medium: Issue of moderate importance requiring prompt attention.
Low: Issue of minor importance requiring attention.

Appendix B

Action Plan

Internal Audit of Information Governance– May 2024

Report Ref.	Risk Area	Advisory Comment	Management Response
4.2.1 (a)	Financial Risk: Fines for non-compliance with legislation.	Consideration should be given to providing Members with Information Governance refresher training.	This will be provided through the refresh of the polices developed by the new Information Governance Team.
4.2.1 (b)	Financial Risk: Fines for non-compliance with legislation.	Following reports of data breaches at other local authorities, consideration should be given to rolling out information governance refresher training to all staff.	This will be developed through the refresh of the polices developed by the new Information Governance Team.
4.2.1 (c)	Financial Risk: Fines for non-compliance with legislation.	Consideration should be given to asking Heads of Service to include data protection risks/the risk of data loss within all service risk registers.	This will be considered as part of the current review of approach to risk management by the Council.
4.3.1 (a)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	Consideration should be given to compiling refresher training (meta pop-ups) on password security and suspicious email links.	This is being considered by the Head of Customer & Digital Services as part of the review of ICT security policy awareness training.
4.3.1 (b)	Legal Risk: Breach of GDPR legislation, Data Protection Act 2018, and the Council's 'information governance framework'.	Consideration should be given to extending the redaction tool software license.	This is a matter for individual services to consider and pay for.

Report Ref.	Risk Area	Advisory Comment	Management Response
4.4.1 (a)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Consideration should be given to compiling training based on the topics requested by officers.	This will be provided through the refresh of the polices developed by the new Information Governance Team.
4.4.1 (b)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Consideration should be given to conducting a 'deep-dive' into home-printing in order to understand the reasons why officers choose (or consider the need) to print from home.	This will be provided through the refresh of the polices developed by the new Information Governance Team, in partnership with the Head of Customer & Digital Services.
4.4.1 (c)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Consideration should be given to permitting the use of Zoom on WDC equipment connected to the network.	This will be provided through the refresh of the polices developed by the new Information Governance Team, in partnership with the Head of Customer & Digital Services.
4.4.1 (d)	Reputational Risk: Reputational damage to the Council arising from data being inappropriately controlled.	Consideration should be given to promoting the active cleansing of staff personal drives.	This will be provided through the refresh of the polices developed by the new Information Governance Team.
4.5.1	Fraud Risk: Data obtained is used for fraudulent purposes.	Consideration should be given to reminding staff not to have deliveries sent to S1 One if they will not be present to accept them.	Work is being progressed around this as part of the overall list of minor issues from the move into S1.