



APPENDIX C(ii)

INTERNAL AUDIT REPORT



DATA MANAGEMENT AND CCTV 2017/18

Issue Date:	Final: 20 th February 2018 Draft: 23 rd November 2017	Issued to:	Richard Ellis – Corporate Services Manager
Author:	Kelly Epps Milda Cufi		Stuart Done – Information and Complaints Officer
			Jonathan Ward - Langman– Commissioning Service Manager
			Beverley Jolly – Corporate Director
			Verina Wenham – Head of Legal and Democratic Services
			Simon Riley – Head of Finance and Corporate Services
			CLr M Rook – Chair of Governance & Audit Committee



DATA MANAGEMENT AND CCTV 2017/18

Executive Summary

1. INTRODUCTION AND OVERALL OPINION

The Data Protection Act 1998 (DPA) requires all organisations that handle personal information to comply with a number of important principles regarding privacy and disclosure. Internal Audit reviewed the Council's procedures and controls to ensure personal data is held and handled in a secure manner and any data loss incidents are suitably reported and acted upon. This also included a review of the management of the Council's CCTV network and compliance with regulations.

General Data Protection Regulations (GDPR) will apply in the UK from 25th May 2018. The Council needs to ensure their implementation plan is finalised and regularly reviewed to confirm the necessary tasks take place promptly.

Policies on data protection, data retention and disposal and ICT security are in place and readily available to staff however Internal Audit testing highlighted that aspects of these policies require updating and roles and responsibilities for officers needs to be clearly defined. Furthermore, compliance with these policies is inconsistent and further communication and training is required to remind officers of where policies can be found and the importance of compliance. Annual online data protection refresher training is mandatory for all employees however 80% of employees in the audit sample had not completed the training within the last 12 months.

A fully complete Information Asset Register was not available at the time of the audit; however there are plans to undertake a full review to capture all data held and produce an Information Asset Register. The Council also needs to ensure the service areas review all their information on an annual basis to ensure that records are being held in compliance with data protection legislation.

Access to paper records are controlled well on and off site, however internal audit identified records held at the off site storage area had not been disposed of in a timely manner once their retention period passed.

Controls over data breach management and access controls for paper records are robust and operating effectively.

The Council's CCTV system comprises of 21 public space cameras installed in Lutterworth and Market Harborough. A comprehensive set of procedure manuals and a Code of Practice have been designed to govern and control the Council's surveillance systems. The Council has been transparent in the use of CCTV cameras by publishing their locations on the website and providing the public with details on how to view their personal information should they wish to do so.

Internal Audit found controls over the security, access, retention and disposal of recorded material were operating well; however a number key controls highlighted in the Code of Practice have not yet been implemented, for example an annual report and audit/compliance checks are yet to be completed.



The audit was carried out in accordance with the agreed Audit Planning Record (APR), which outlined the scope, terms and limitations to the audit. The auditor's assurance opinion is summarised in the table below:

Internal Audit Assurance Opinion			
Control Environment	Satisfactory ●		
Compliance	Limited ●		
Organisational Impact	Moderate ●		
Risk	Essential	Important	Standard
01 - Poor governance arrangements over the management of data and lack of staff training, leading to non compliance with the Data Protection Act (DPA).	2	2	2
02 - Records are not created or maintained accurately, leading to non-compliance with the Data Protection Act and reputational damage.	2	2	0
03 - Unauthorised access to the Council's records leading to possible data breaches, financial penalties and reputational damage.	0	1	0
04 - Failure to recognise and respond to individuals' requests for access to their personal data resulting in potential fines and reputational damage.	0	0	1
05 - Lack of transparency over the use of a CCTV system leading to reputational damage and poor public perception.	0	0	2
06 - Poor governance arrangements leading to non compliance with data protection legislation and the Surveillance Camera Commissioner's Code of Practice.	0	1	1
Total Number of Recommendations	4	6	6



2. SUMMARY OF FINDINGS

Risk 1: Poor governance arrangements over the management of data and lack of staff training, leading to non compliance with the Data Protection Act 1998.

By processing personal data the Council must record the types of data it holds and why on the public register of data controllers. This is called 'registration', which is renewed and updated annually. Harborough District Council's registration with the Information Commissioner is valid and will expire on 12th November 2018. If a Councillor processes personal data in relation to their constituency casework when representing members of their ward they become a data controller. The Council reminds Councillors of this requirement and current records confirm that 24% of Councillors were registered as Data Controllers with the ICO.

The Information Commissioner's Office (ICO) advises that a standalone policy statement or a general staff policy on data protection should be in place. In April 2017, the Council created an Information Governance Policy that provides an over-arching framework which sets out how the Council manages its information assets. This policy is supported by a number of policies and guidance notes including Data Protection Guidance that was created in April 2013. No amendments to the guidance have been made since 2013 because the principles of data protection have not changed, however the guidance should be subject to a formal review at regular intervals to ensure it covers current practice and any changes in legislation. **(See recommendation 1)**

It is good practice to identify a person or team with day-to-day responsibility for developing, implementing and monitoring a data protection policy and from the 25th May 2017, GDPR will require the Council to have a Data Protection Officer (DPO) At the time of the audit a DPO has not been appointed and the Data Protection Guidance states the DPO is a member of staff who no longer works for the Council. **(See recommendation 2).**

It is mandatory for all employees to be trained in basic data protection principles. This is included in the corporate induction course through the Council's e-learning package, Learning Matters, and refresher training should be completed every twelve months. Internal Audit checked a sample of 25 employees and found that 24 (96%) had completed data protection training however only a third of these employees had undertaken training within the last twelve months. In addition, communications such as intranet articles, posters, circulars, and team briefings are not regularly carried out and would assist in maintaining awareness of the data protection principles. **(See recommendation 3 and 6)**

The seventh principle of the DPA requires that personal data is protected by appropriate security measures. In order to decide what level of security is right for an organisation the risks to personal data need to be assessed. The Corporate Director (Resources) is considered to be the Senior Information Risk Officer (SIRO) although data protection guidance and the Information Governance Policy do not define the roles and responsibilities of the SIRO. **(See recommendation 4)**

In order to keep up to date with changes in relevant legislation, the Information and Complaints Officer attends monthly Strategic Information Management Group meetings that are attended by agency representatives from across the county.

The GDPR will apply to the UK from 25th May 2018 and the Council has produced a GDPR Gap Report to acknowledge the changes coming into force and recognise what work is required. At the time of the audit the Information and Complaints Officer was in the process of compiling an implementation plan. This needs to be actioned as a matter of priority. **(See recommendation 5)**



Privacy notices will be made a legal requirement as part of GDPR. The Council's website contains a Fair Processing Notice that explains how personal data will be used and for any queries on data use and sharing, the contact details of the Information and Complaints Officer are provided. Also privacy notices are included on the various forms and templates.

Risk 2: Records are not created or maintained accurately, leading to non-compliance with the Data Protection Act and reputational damage.

The Council does not have an assigned records management lead. Overall responsibility for managing records lies with service areas. There is a Document Retention Policy dated 2017 available to staff outlining the retention periods for various categories of information, although the 2012 version is published on the intranet. The policy sets out the organisation's approach to records management in terms of data retention and disposal however roles and responsibilities for implementing the policy and monitoring compliance are not defined. **(See recommendations 1 and 4)**

It is necessary to know what data is held and how, in order to ensure that personal data is managed effectively and securely. A record of information held by each service area is available, although the list was compiled to recognise what data needs to be made public and whether it is up to date. The Information and Complaints Officer has planned to undertake a full information audit to capture all the data held which will form an Information Asset Register **(See recommendation 7)**

The ICO recommend that organisations carry out regular exercises to identify, assess and manage records management risks in order to identify what might go wrong with a process and why. Measures can then be put in place to mitigate these risks. Internal audit reviewed the Risk and Opportunity register and found risks associated with loss of data from a business continuity perspective, however records management risks were not included. These might include records not being updated, not being destroyed in a timely manner or not being held securely. **(See recommendation 8)**

The Council has an off site, secure storage area, managed by an external provider. Archived papers records are stored at this location and there is an inventory available. Internal Audit selected a sample of 17 boxes due for disposal and three that were not due. The company's representative explained that they do not dispose of data unless requested by the Council, and no such requests had been made since the Council transferred the boxes on 20th August 2016. Of the sample of records selected which should have been disposed of, none had been disposed of and all were still held at the storage area. Furthermore, one of these boxes contained taxi licensing applications with personal sensitive information and in some cases copies of actual DBS certificates which must not be retained by the Council for any period of time under data protection legislation. **(See recommendation 9)**

Internal audit reviewed five service areas and checked that data in each of the areas is being retained in accordance with council policy. The review revealed that recent reviews of the records held had not been conducted, nor are regular reviews taking place. Also interviews with officers highlighted that officers were not clear on the data retention guidelines and there was a lack of awareness of the records held in the off-site storage area. **(See recommendation 10).**



Risk 3: Unauthorised access to the Council's records leading to possible data breaches, financial penalties and reputational damage.

The Council has an up to date ICT Security Policy which is accessible to all employees covering use of laptops and other portable ICT devices within and outside of the Symington Building. It aims to ensure adequate protection of the Council's ICT assets, people, programs, data and equipment, on a cost effective basis, against any threat which may affect their security, integrity and/or the level of ICT service required by the Council to conduct its business.

There is an ICT Removable Media Policy which was last reviewed and updated in September 2014. The policy prohibits the use of all removable media devices. The use of removable media devices are only approved if a valid business case for its use is provided.

The ICT Email Security policy confirms the Council monitors e-mail traffic by automated means and e-mail is stored centrally to enable further audit, if necessary. The content of e-mail (including attachments) is also subject to monitoring and filtering policies and officers with a requirement to access and use sensitive information have an additional mailbox (GCSX – GovConnect Secure eXtranet) so that they can send and receive e-mail securely.

The Council has established a process to assign user accounts to authorised individuals, and to manage user accounts effectively to provide the minimum access to information. Each user is assigned their own username and password to ensure accountability and appropriate password security procedures and 'rules' exist for the Council's network.

It is important to establish entry controls to restrict access to premises and equipment and prevent unauthorised physical access, damage and interference to personal data. The Council has implemented entry controls to buildings so that access is restricted on a need to know basis only. An ID badge/access card system is in operation for staff, contractors and visitors. Closed circuit television (CCTV) is in operation and protocols are in place for controlling visitors to the building. Internal Audit reviewed 25 swipe cards and found that four card owners no longer worked at the Council, however their cards remain active. The four named individuals were unknown to HR and internal audit were unable to confirm their exact leave date, however all cards had not been used for at least eight months. Officers deactivated these cards during the audit. **(See recommendation 11)**

The Council aims to operate electronically and encourages paper light working however the Information Governance Policy states that any sensitive paper based records must be protected by adequate security measures. A review of records in five service areas demonstrated that paper records are kept in lockable filing cabinets.

Electronic records should be stored securely with higher levels of security for sensitive personal data. The Council uses the DMS system to store most electronic data. The system does have potential to be used as a records management system which would assist in document retention and timely disposal. A review of records held by five service areas highlighted that some bespoke systems are being used for the processing and storage of records, as well as the DMS system and network folders. Internal Audit reviewed access to the active directory, relevant network folders in the sample and to the DMS and found that access appeared appropriate however 8% of DMS system users were no longer current members of staff. **(See recommendation 10)**

An Information Security Clear Desk and Clear Screen Policy is available for members of staff on the Intranet. The policy sets guidelines to reduce the risk of a security breach caused by documents left unattended in shared workspaces on the premises. It covers the information used in paper and electronic formats, as well as the removable media. The service managers should occasionally be checking their areas making sure no sensitive data is left unattended however there are no regular checks conducted to ensure compliance. **(See recommendation 10)**



Data security breaches may arise from a theft, an attack on Council systems, the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure. When a breach occurs it is important that it is dealt with effectively and appropriate action is taken to avoid it happening again in the future. Of five reported data breaches, two were selected for review and both had been handled in accordance with the Council's Data Loss Procedure.

Processes to securely dispose of records and equipment when no longer required have been established. The ICT Removable Media Policy states that removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. A third party specialist accredited data destruction company is used to dispose of any equipment. Staff are provided with the disposable bags for larger quantities of disposable confidential data and shredders are also available. Discussions with the officers from five service areas confirmed that confidential bins, shredders, confidential waste sacks are used for disposals.

Risk 4: Failure to recognise and respond to individuals' requests for access to their personal data resulting in potential fines and reputational damage.

The Data Protection Act 1998 (DPA) gives individuals the right to find out what personal data the Council holds about them, why the information is held and who it is disclosed to. This right is exercised by making a written subject access request (SAR) to the Council.

The Information and Complaints Officers has received appropriate training on subject access requests and is responsible for logging all subject access requests and co-ordinating responses with assistance from two Administrators. A flowchart and data protection guidance describe the process of receiving and responding to the data subject access requests.

Guidance on making a SAR, along with a form, is available on the organisation's website. It advises that those making a request may be required to attend the Council offices with further proof of identification in order establish their identity before request is processed. It states that the Council will respond to all requests within 20 working days even though the requirement is 40 calendar days and can charge a fee that it is considered reasonable for making information available.

All SARs are logged on a manual spreadsheet. There have been 44 requests since 1st January 2017 and Internal Audit selected a sample of eight requests for review. Testing highlighted the following:

- Each request is assigned a unique reference number.
- Original requests were seen and were responded to within 20 working days.
- No use was made of the SAR checklist in any of the cases which required one and therefore an audit trail confirming identification was verified was not available.
- One written response included incorrect reference to the Freedom of Information Act.
- Currently the responses sent out do not include the information on what searches were made in order to obtain the required information.

(See recommendation 12).



Risk 5: Lack of transparency over the use of a CCTV system leading to reputational damage and poor public perception.

The Council has taken steps to ensure the use of CCTV cameras is as transparent as possible. Contact details for access to CCTV information are available on the Council's website. There are 19 CCTV locations throughout Market Harborough and Lutterworth and their locations are published on the Council's website. Internal Audit visited 15 CCTV cameras on 5th October 2017 and found that four of these cameras did not have signs displayed indicating the presence of CCTV monitoring, one sign was placed too high and unreadable, and signage for one camera did not provide the correct contact details. **Recommendation 13** addresses this issue. All other signs viewed by Internal Audit were however clear, visible and readable, indicating that CCTV is in operation and contact details for the Council were provided.

A Privacy Impact Assessment has not been conducted and documented to consider the CCTV scheme's impact on people's privacy. It has been noted by the service that an assessment must be completed for any new cameras or changes to the current coverage. It is noted that consultation with the Community Safety Partnership was undertaken when the new code of practice was produced. Impact on privacy must be subject to formal review and consultation should any cameras be added, removed, changed or upgraded. No formal recommendation has been made at this time.

The Council's code of practice for CCTV requires the Council's surveillance system to be evaluated at least every two years, including a review of aims and objectives and whether the CCTV is meeting those objectives. It also states that an annual report will be produced, however this has not yet been completed and there are plans to have this done by the end of 2017. **See recommendation 14.**

Risk 6: Poor governance arrangements leading to non compliance with data protection legislation and the Surveillance Camera Commissioner's Code of Practice.

An up to date Code of Practice for the operation of the CCTV system in Market Harborough and Lutterworth is in place and supported by a clear, documented procedure manual. All documents describe how information should be handled in practice and provide guidance on disclosures and record keeping. Individuals who have any involvement with the CCTV systems are required to sign to confirm they have read and understood both documents and Internal Audit confirmed that all nine CCTV operators have signed.

A fully comprehensive training programme has been developed for CCTV operators and Internal Audit found all operators to be properly trained or in the process of completing their training programme. Operators are awarded a BTEC intermediate award in CCTV PSS (a licence to practice) covering CCTV control room principles and practices as well as relevant legislative provisions relating to human rights, privacy, equalities and other legislation affecting individual rights.

The CCTV Control room is based at Market Harborough Police Station and all operators are subject to police background and security clearance checks. During a visit to the CCTV control room on 12th October 2017 it could be seen that access to the control room is secure and only accessible via a valid swipe card. All visitors to the control room must sign a visitors log confirming arrival and departure time and reason for visit.

A retention period of 28 days has been set for all recorded information, unless it is required for evidence. A visit to the CCTV Control Room confirmed that CCTV footage was being retained for the appropriate number of days. Any discs created for evidence which have not been collected within 60 days of its production will be securely destroyed;



however a review of the evidence folder confirmed the oldest CD to be approximately four months old. **Recommendation 18** will address this issue.

Information can be disclosed to the police for evidential purposes and this is carried out in a controlled manner using a CCTV database. Each entry on to the log is given a unique reference number and sufficient information regarding the search is recorded, including who requested it, who completed it, the outcome and the date and time the information was downloaded. An audit trail exists to confirm when the evidence was handed over to the police and to whom it was passed. Should the evidence not be required the information is disposed of securely.

People and organisations other than the police make enquiries about CCTV images. The public are suitably made aware on the Council's website of how they can make a subject access request (SAR), who it should be sent to and what information needs to be supplied with their request.

SARs are logged and captured in the same way that any other request is made therefore it was not possible during the audit to distinguish between different types of requests and officers stated they were unable to produce a report from the CCTV database showing all requests in a given time period. **See recommendation 15**

Regular audits or checks to ensure compliance with the Code of Practice and supporting procedure manual are not currently take place. **See recommendation 16**

3. LIMITATIONS TO THE SCOPE OF THE AUDIT

This is an assurance piece of work and an opinion is provided on the effectiveness of arrangements for managing only the risks specified in the Audit Planning Record.

Our work does not provide absolute assurance that material error; loss or fraud does not exist. The review did not include data sharing or Freedom of Information requests.

4. ACTION PLAN

The following Action Plan provides a number of recommendations to address the findings identified by the audit. If accepted and implemented, these should positively improve the control environment and aid the Council in effectively managing its risks.



ACTION PLAN

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
Risk 1: Poor governance arrangements over the management of data and lack of staff training, leading to non compliance with the Data Protection Act 1998.						
1	<p>Policies and guidance documents relating to data protection and records management were found to be out of date in some instances and not reviewed at regular intervals.</p> <p>There is a risk that correct procedures are not followed potentially leading to non compliance with data protection legislation.</p>	<p>Review current data protection policies, codes of conduct and training to ensure these are consistent with the new requirements arising from the GDPR.</p> <p>All Data Protection policies should be subject to a formal review every 2-3 years and updated where necessary.</p> <p>Review dates should be recorded on the policy documents.</p>	<p>All relevant policies currently being reviewed in readiness for GDPR.</p> <p>The action plan has been implemented and will be substantively in place in readiness for the 25/05/2018 GDPR deadline.</p> <p>DP Policy register to be established to ensure refresh dates are not missed.</p> <p>Horizon scanning required to keep abreast of key changes to legislation.</p> <p>Draft DP Bill still going through Parliament. Some policy changes will be required if it is enacted as is. Dates to be confirmed.</p>	<p>Standard</p> <p style="color: green; font-size: 20px;">●</p>	<p>Information Governance Officer</p>	<p>31 May 2018</p>

2	<p>The Council has not appointed a Data Protection Officer (DPO) with day-to-day responsibility for developing, implementing and monitoring a data protection policy.</p> <p>This is a requirement of the General Data Protection Regulations (GDPR).</p>	<p>A Data Protection Officer should be appointed.</p> <p>The key responsibilities of a DPO are:</p> <ul style="list-style-type: none"> • To inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection laws. • To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. • To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc). 	<p>The Information and Complaints Officer to be designated as DPO. The role has been reviewed and job evaluation is being finalised. This action will be complete before it is required for the GDPR deadline.</p>	<p>Essential</p> <p>●</p>	<p>Corporate Director(s)</p>	<p>28 February 2018</p>
3	<p>Internal Audit checked a sample of 25 employees and found that 24 (96%) had completed data protection training however only a third of these employees had undertaken training within the last 12 months.</p>	<p>All staff should be required to complete Data Protection Awareness online training on an annual basis. This could be checked by Line Managers as part of the annual appraisal process.</p>	<p>All staff sessions on GDPR to be held as well as service specific sessions. Online training module to be reviewed and updated. Will this be complete before 31st May. Annual refresh training (through Learning matters) to be enforced.</p>	<p>Important</p> <p>●</p>	<p>Information Governance Officer</p>	<p>31 May 2018</p>

4	<p>The roles and responsibilities of responsible officers for data management are not clearly defined in relevant Council policies and procedures, such as the Senior Information Risk Officer (SIRO), Data Protection Officer and records management lead officer.</p> <p>Without clear accountability and communication of individual responsibilities for data management, there is a risk that data is not retained in accordance with Council policy and data protection legislation.</p>	<p>Individual roles and responsibilities for data protection and records management should be clearly defined in the Council's Data Protection Policy and the Document Retention Policy.</p> <p>Allocated roles should be communicated effectively to those individuals that are impacted.</p>	<p>Agreed – roles and responsible officer(s) to be defined.</p> <p>Tentative date for all staff briefing scoped and online learning module agreed for roll out following that briefing.</p> <p>Members briefing to take place in or before group sessions. Date scoped but yet to be agreed.</p>	<p>Important</p> <p>●</p>	<p>Corporate Services Manager</p>	<p>30 April 2018</p>
5	<p>The Council's GDPR implementation plan has not yet been finalised.</p> <p>Without an agreed action plan, there is a risk that objectives are not achieved in a timely manner leading to non compliance with the General Data Protection Regulations.</p>	<p>The Council's GDPR implementation plan should be finalised and implemented to ensure the Council is fully prepared when the regulations come into force on 25th May 2018.</p>	<p>Plan in place with key targets and tasks identified.</p> <p>Policy changes have been drafted and data collection exercises are underway with regards to providing future compliance data on the state of compliance.</p> <p>GDPR creates new obligations for measurement and quantification of DP (Data Protection) compliance. The work plan will ensure this happens to meet the coming in to force date.</p> <p>Progress of compliance implementation to be monitored through the Programme Board.</p>	<p>Essential</p> <p>●</p>	<p>Information Governance Officer</p>	<p>31 May 2018</p>

6	Internal Audit did not see evidence of regular communication of key messages to reinforce data protection training and maintain awareness.	The Council should consider introducing regular communications of key messages to help reinforce data protection training and maintain awareness (for example, intranet articles, circulars, team briefings and posters).	<p>To be introduced/reinforced as part of preparations for GDPR.</p> <p>This will also form part of whole organisation and team briefings. i.e. the communication of key messages and differences between the current and future DP regimes.</p> <p>There will be a renewed annualised requirement to repeat certain training requirements in order to positively move the organisational culture to one which is acutely aware of DP issues.</p> <p>Recommendations:</p> <ul style="list-style-type: none"> • Regular items, (Core Brief) • Team training • Splash pages on the intranet • 1-2-1's where appropriate. • Visual reminders (Posters) 	Standard ●	Information Governance Officer	30 April 2018
---	--	---	--	-------------------	--------------------------------	---------------

Risk 2: Records are not created or maintained accurately, leading to non-compliance with the Data Protection Act and reputational damage.						
7	<p>A fully complete Information Asset Register (IAR) was not in place at the time of the audit.</p> <p>The Information and Complaints Officer has plans to undertake a full review to capture all data held and produce an Information Asset Register.</p> <p>An IAR is a key tool for fully exploiting the Council's information assets – it helps identify areas of duplication and encourages greater efficiency. It can be used to spot areas of potential risk – e.g. loss of personal data. By understanding the nature of its information and where it is held, the Council can manage these risks more easily.</p>	<p>An information audit or records survey should be completed in order to produce an Information Asset Register.</p> <p>Each asset should have an Information Asset Owner (IAO). This is the individual responsible for ensuring that the risks to, and the opportunities for, the asset are monitored.</p> <p>There are a number of fields which should be recorded on the IAR – e.g. how long assets should be retained, who can access them and whether they contain personal data. Assets can be described and managed at a system level if the information contained within the system is the same – e.g. a purchase order database. If systems contain various types of information with different values, risks and sensitivities, each should be noted as a separate information asset.</p>	<p>Information Assets Register being reviewed/updated as part of preparation for GDPR. This will be in place for the GDPR deadline.</p> <p>Current data sets do not meet the requirements of GDPR.</p> <p>A new interrogative spreadsheet has been set up to draw together the elements of recorded data processing, asset detail, retention guidelines, responsible officer and justification for processing. Once completed by all services, HDC will have a comprehensive IAR which will form the basis of future compliance audits and data classification exercises.</p>	<p>Essential</p> <p>●</p>	<p>Information Governance Officer</p>	<p>30 April 2018</p>

8	<p>Risks associated with loss of data from a business continuity perspective are highlighted on the Council's Risk and Opportunity Register, however, data protection and records management risks are not recorded or monitored through the corporate risk management process.</p> <p>There is a potential risk that information risks are not mitigated or managed effectively, leading to potential data breaches.</p>	<p>The Council should:</p> <ol style="list-style-type: none"> 1) incorporate information risk(s) in to the corporate risk and opportunity register; and 2) Regularly assess and update, treat, tolerate or mitigate risks as appropriate. 	<p>Agreed.</p> <p>Information risk assessments to be conducted for all new projects. This will also include conducting of DPIA (Data Protection (Privacy) Impact Assessments.</p> <p>Privacy by design will be embedded in the organisation which will mitigate the risks to personal data. This will involve the scrutiny of contracts and systems to ensure that the HDC is satisfied as their suitability of function.</p> <p>Risks to be identified and monitored through the corporate risk monitoring process.</p>	<p>Important</p> <p>●</p>	<p>Corporate Services Manager</p>	<p>30 April 2018</p>
9	<p>Internal audit selected a sample of 20 boxes from the Council's off site storage area. Testing highlighted that 17 of the boxes were due for disposal and had not been destroyed.</p> <p>Furthermore, one box contained taxi licensing applications that had personal sensitive information including actual DBS certificates. These should have been destroyed in December 2016 and no DBS certificates should be retained for any period of time.</p>	<p>Records held in the off site storage area should be reviewed as soon as possible to ensure that records due for disposal are destroyed.</p> <p>Any DBS certificates held must be securely destroyed.</p>	<p>Responsibility of relevant service manager. All service managers to be required to carry out periodic reviews of all data including information held off-site.</p> <p>A programme of inspection to be established to ensure that the data held, is disposed of, retained or at least inspected in line with the requirement of both the legislation and internal policies.</p>	<p>Essential</p> <p>●</p>	<p>Service Managers</p>	<p>At least annually</p>

10	<p>Internal audit reviewed five service areas and checked that data in each of the areas is being retained in accordance with Council policy.</p> <p>Testing highlighted that reviews of the records held have not been conducted, nor are regular reviews taking place.</p> <p>Furthermore, interviews with officers highlighted that officers are not clear on the data retention guidelines and there was a lack of awareness of the records held in the off-site storage area.</p> <p>There is a risk of not complying with the fifth data protection principle: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".</p>	<p>The Data Protection Officer should remind all Information Asset Owners to review their data at least annually to ensure that records are being held in accordance with data protection legislation.</p> <p>Information Assets Owners should be reminded of the Council's Document Retention Policy.</p> <p>The Data Protection Officer should perform ad-hoc spot checks to ensure that policies are being complied with.</p>	<p>Agreed.</p> <p>Part of the process of gathering the information to populate the IAR (Information Asset Register) will allow these documents to be a living document which should be reviewed and updated on a continual basis.</p> <p>It will form the basis of a compliance check which will involve the regular auditing of each service as part of the wider compliance checking program.</p> <p>Inspection forms have been created in anticipation of this requirement.</p> <p>A data classification exercise will also result from this exercise.</p>	<p>Important</p> <p>●</p>	<p>Information Governance Officer</p>	<p>31 July 2018</p>
----	---	--	---	---------------------------	---------------------------------------	---------------------

Risk 3: Unauthorised access to the Council's records leading to possible data breaches, financial penalties and reputational damage.

11	<p>Internal audit reviewed a sample of 25 swipe cards enabling access to the Council's Symington Building. Testing confirmed that four live cards belonged to individuals who no longer work at the Council.</p> <p>All four cards were deactivated during the audit.</p> <p>Failure to deactivate ID cards in a timely manner could put the Council at risk of unauthorised access to sensitive and confidential data.</p>	<ol style="list-style-type: none"> 1. Review the procedure for deactivation of access cards when staff leave, including notification of deactivation and collection of ID badges. 2. Audit the card system to ensure it matches the current employment record in HR. 3. Review the temporary access card procedure to ensure all cards are accounted for and robust system of issue and collection of cards, including revoking access in a timely manner. 	<p>There is a process in place to do this as part of leavers notifications.</p> <p>There is a leavers process for both physical and systemic entry to HDC systems. This needs to be checked on a regular basis to ensure compliance.</p> <p>Responsible service manager aware of the requirement.</p>	<p>Important</p> <p style="text-align: center;">●</p>	<p>Facilities Officer</p>	<p>31 March 2018</p>
----	---	---	---	---	---------------------------	----------------------



Risk 4: Failure to recognise and respond to individuals' requests for access to their personal data resulting in potential fines and reputational damage.

12	<p>Internal Audit testing of eight Subject Access Requests highlighted the following:</p> <ul style="list-style-type: none"> No use was made of the SAR checklist in any of the cases which required one and therefore an audit trail confirming identification was verified was not available. One written response included incorrect reference to the Freedom of Information Act. Responses sent do not include the information on what searches were made in order to obtain the required information. 	<p>Officers should be reminded of the following when responding to Subject Access Requests:</p> <ul style="list-style-type: none"> The SAR checklist list must be completed in all cases to ensure that necessary steps have been completed e.g. identification verification. Standard templates should be used for all SAR responses. <p>The Data Protection Officer should carry out ad hoc spot checks on SAR requests to ensure that procedures are being complied with.</p>	<p>The requirements of the SAR checklist are being met.</p> <p>There are no checklists for 'SAR' related requests which formed 7 of the 8 sets examined. These are inter-agency requests formulated under s29 and 35 of the Data Protection Act 1998. The requirements for personal identification are not the same.</p> <p>Completion of checklist to be enforced to evidence compliance in all other SAR cases.</p> <p>SAR process form has been revised for GDPR and includes check list to comply with A15.</p> <p>Existing DPA SAR form is in use until 25/05/2018, but does contain checklist. Receiving officer to note what proofs have been provided where required.</p>	Standard ●	Information Governance Officer	With immediate effect
----	---	--	---	-------------------	--------------------------------	-----------------------



Risk 5: Lack of transparency over the use of a CCTV system leading to reputational damage and poor public perception.

13	<p>Internal Audit visited fifteen locations on 5th October 2017 and found that there was no signage for CCTV cameras 1, 2, 3, and 9.</p> <p>Camera 5 is placed in a car park however signage is placed too high making it unreadable.</p> <p>Signage for camera no. 15 did not have the correct contact details.</p> <p>Without suitable signage, individuals may be unaware that they are in an area where CCTV cameras are being used.</p>	<p>The Council should place clear, readable signage on all cameras to let people know when they are in an area where a surveillance system is in operation.</p>	<p>Agreed.</p>	<p>Standard ●</p>	<p>Commissioning Service Manager</p>	<p>31st May 2018</p>
----	---	---	----------------	-----------------------	--------------------------------------	---------------------------------

14	An annual review has not been conducted on the Council's CCTV system to ensure that it is still doing what was intended to do so.	The Council should conduct a review, at least annually, of the CCTV system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified.	Agreed.	Standard 	Commissioning Service Manager	31 st May 2018
Risk 6: Poor governance arrangements leading to non compliance with data protection legislation and the Surveillance Camera Commissioner's Code of Practice.						
15	Officers were unable to produce a report showing all subject access requests received in a given time period. Also SARs are not uniquely identifiable and are treated in the same way as any other request. Internal Audit were therefore unable to verify that subject access requests for CCTV images are handled in accordance with data protection legislation.	<ol style="list-style-type: none"> 1. Subject access requests should given a unique reference so they can be easily identified. 2. Officers should investigate whether a report can be produced from the CCTV database. 3. A clear audit trail should be retained for all SARs e.g. original request, confirmation of ID and response sent to requester. 	These requests should be channelled through the usual information access process. A reference will be allocated at that point.	Important 	Commissioning Service Manager	31 st May 2018



16	<p>Regular audit/checks of current CCTV processes and procedures are not currently in operation.</p> <p>There is a risk that procedures are not complied with, potentially leading to non compliance with data protection legislation.</p>	<p>As per the Surveillance Camera Code of Practice, there should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.</p>	<p>Agreed.</p>	<p>Standard ●</p>	<p>Commissioning Service Manager</p>	<p>31st May 2018</p>
----	--	--	----------------	-----------------------	--	-------------------------------------

GLOSSARY

The Auditor's Opinion

The Auditor's Opinion for the assignment is based on the fieldwork carried out to evaluate the design of the controls upon which management rely and to establish the extent to which controls are being complied with. The tables below explain what the opinions mean.

Compliance Assurances		
Level	Control environment assurance	Compliance assurance
Substantial ●	There are minimal control weaknesses that present very low risk to the control environment.	The control environment has substantially operated as intended although some minor errors have been detected.
Good ●	There are minor control weaknesses that present low risk to the control environment.	The control environment has largely operated as intended although some errors have been detected.
Satisfactory ●	There are some control weaknesses that present a medium risk to the control environment.	The control environment has mainly operated as intended although errors have been detected.
Limited ●	There are significant control weaknesses that present a high risk to the control environment.	The control environment has not operated as intended. Significant errors have been detected.
No ●	There are fundamental control weaknesses that present an unacceptable level of risk to the control environment.	The control environment has fundamentally broken down and is open to significant error or abuse.

Organisational Impact		
Level	Definition	
Major ●	The weaknesses identified during the review have left the Council open to significant risk. If the risk materialises it would have a major impact upon the organisation as a whole.	
Moderate ●	The weaknesses identified during the review have left the Council open to medium risk. If the risk materialises it would have a moderate impact upon the organisation as a whole.	
Minor ●	The weaknesses identified during the review have left the Council open to low risk. This could have a minor impact on the organisation as a whole.	

Category of Recommendations

The Auditor prioritises recommendations to give management an indication of their importance and how urgent it is that they be implemented. By implementing recommendations made managers can mitigate risks to the achievement of service objectives for the area(s) covered by the assignment.

Priority	Impact & Timescale
Essential ●	Action is imperative to ensure that the objectives for the area under review are met.
Important ●	Requires actions to avoid exposure to significant risks in achieving objectives for the area.
Standard ●	Action recommended to enhance control or improve operational efficiency.