

INTERNAL AUDIT REPORT

FROM: Audit & Risk Manager
TO: Deputy Chief Executive (AJ)
C.C. Chief Executive
Head of Finance
Democratic Services Manager
Information Governance Manager
Portfolio Holder (Cllr Day)

SUBJECT: Information Governance
DATE: 31 March 2021

1 Introduction

- 1.1 In accordance with the Audit Plan for 2020/21, an examination of the above subject area has recently been completed by Ian Davy, Principal 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.
- 1.3 The audit was undertaken during the COVID-19 pandemic. This has meant a slightly different approach has been taken to complete the audit. Rather than observing staff members and meeting staff face to face, correspondence has been via email or Teams video calls.

2 Background

- 2.1 The original scope for this audit was for a review to be performed of what was being left on desks by staff at the end of each day. However, due to the COVID-19 pandemic and the resulting changes to the way everyone was working, this was not appropriate.
- 2.2 Instead, a review has been performed on how staff are dealing with data security in their new working environment, be that at home or within Council premises, and how data security was maintained during the mothballing of parts of Riverside House and the clearance of other levels to allow for a COVID-safe environment to be put in place for those that needed to work from the office.

3 Scope and Objectives of the Audit

- 3.1 The audit was undertaken through two main 'avenues', firstly through discussion with relevant staff to ascertain how information governance as a whole had been managed, including the mothballing process followed at Riverside House and, secondly, via a staff survey to identify whether staff

working from home were dealing appropriately with the security of data that they obtained. Some of these aspects were also discussed with staff from the relevant teams (e.g. the Corporate Support Team (CST)).

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

- Training and guidance
- Data use and retention
- Data disposal.

3.3 The control objectives examined were:

- Staff are aware of how to deal with data they obtain in different working conditions
- Information is not unwittingly disclosed to other staff or contractors
- Information is not unwittingly disclosed by staff working from home
- Personal / sensitive data continues to be disposed of in an appropriate manner during COVID working conditions.

3.4 A separate audit of Income Receipting and Document Management has also recently been completed that covered other aspects of the work of the CST. Whilst there is some overlap (and some recommendations from that audit relate to information governance), this audit is concerned with topics relating specifically to data security.

4 Findings

4.1 Recommendations from Previous Reports

4.1.1 Due to the specific nature of this audit, the recommendations from the previous audit of Information Governance undertaken in May 2018 were not followed up.

4.2 Training & Guidance

4.2.1 The Information Governance Manager (IGM) advised that there had been no specific training provided to staff in relation to information governance whilst working from home (WFH). However, he suggested that work was being undertaken on preparing some (general) data protection presentations which will be delivered to managers at both Warwick and Stratford before being made available to all staff as recordings on the intranet.

4.2.2 The Democratic Services Manager & Deputy Monitoring Officer (DSM) confirmed that no WFH-specific training had been delivered although meta 'training' and intranet notices have been pushed out.

4.2.3 The Learning & Development Officer confirmed that eleven 'meta' notices / training items had been pushed out over the last year with the list including some directly relevant 'notices' as well as others that deal with the processing of data (e.g. NFI).

4.2.4 As part of the staff survey, specific questions were asked of staff as to what they had received, or felt they needed, in terms of training or guidance for their new ways of working. A summary of the 'findings' from the staff survey

are covered in 4.5 below, with a more detailed summary of the responses in Appendix B.

- 4.2.5 As highlighted in other sections of this report, some data protection 'issues' have been communicated to staff over the course of the last year and the IGM agreed that it may be a good idea to put together guidance in the form of a 'crib sheet' of issues that staff need to be aware of.

Risk

Staff may not be aware of data protection issues that impact their way of working.

Recommendation

A guidance document, pulling together all issues identified, should be drawn up and distributed to all staff.

- 4.2.6 The IGM highlighted that all relevant policies should apply - no matter where a member of staff is working. He confirmed that the policies had been reviewed shortly before he joined the Council and that he had no concerns over their suitability. However, he suggested that there may be a need for a specific homeworking policy should this continue to be the norm.
- 4.2.7 As part of the staff survey, specific questions were asked of staff as to whether they were aware of policies / procedure documents relevant to their new / current ways of working (see 4.5 and Appendix B).
- 4.2.8 The IGM and the DSM both suggested that there had not been 'regular' communications regarding data security issues. However, there had been occasional notices posted on the intranet as and when there was a specific need, such as the auto-completion of email addresses and use of 'connected devices'. The DSM also suggested that more was needed around requests for changing personal data.
- 4.2.9 As part of the staff survey, specific questions were asked of staff as to whether they had received or were aware of any communications relating to data-related issues that have occurred due to home working / current working (see 4.5 and Appendix B).
- 4.2.10 The DSM advised that all staff visiting Riverside House to clear their offices had to arrange the visits through the Building Surveyor (BS) or the Temporary Riverside House Building Manager (TBM). After one 'near miss', all paperwork to be disposed of was placed into a secure room before 'volunteers' went through the contents to remove any 'non-paper' items (e.g. folders) with the paperwork subsequently being collected for off-site secure destruction. As such, there was no general need to provide guidance to all staff in relation to the office clearance.
- 4.2.11 The BS advised that, with the exception of the main GDPR training, no specific guidance was issued to him for the mothballing process (and the clearing of paperwork from other levels) although this was likely due to the fact that he had raised queries through the Workforce Steering Group directly

in relation to data security; it was therefore probable that there was no perceived need for further guidance to be issued.

4.3 **Data Use & Retention**

- 4.3.1 Whilst the majority of staff are now working from home, a small number of staff are working from Riverside House, either because their work requires them to be in the office, or there are 'wellbeing' issues. The 'set-up' of Riverside House has been amended to allow for COVID-safe working practices, with staff sat in different areas of the building compared to their previous office base. As a result, staff may now hear or see different information than they would have previously.
- 4.3.2 The DSM advised that the Perspex screens in place at each desk have had an effect on the way that sound transmits around the office although "only 50% of the conversations are heard".
- 4.3.3 The DSM also highlighted that the new arrangements have actually fostered new team dynamics. The IGM also suggested that there was a need to ensure that staff did not feel isolated in the office, as this was one of the reasons that some staff are actually working at Riverside House.
- 4.3.4 Both the DSM and the IGM confirmed that staff were still respecting data security as they would have done in the office previously.
- 4.3.5 Due to the need to ensure that the offices were safe to work in, the contract cleaners were in attendance more frequently than before. The IGM agreed that there was a higher risk of cleaners being in the offices during the day and, as such, there was a need to consider the data security practices of the contractor, ensuring that they (as a contractor as opposed to individual staff members) deal with any data appropriately.
- 4.3.6 The DSM suggested that the cleaners were, however, only approaching desks when staff were not at them (with the use of laminated signs to advise the cleaners whether they were free for cleaning) and staff should be ensuring that no data was visible.
- 4.3.7 The Contract Services Manager obtained confirmation from Churchill (the cleaning contractor) that their staff have to sign a confidentiality agreement as part of their application which includes:
- During the course of your employment you may see, hear or have access to information on matters of a confidential nature relating to Churchill Contract Services, their employees and their clients. Under no circumstances should such information be divulged or passed on to any other unauthorised person(s) or organisations. This includes divulging the nature of ours or our client business.
- 4.3.8 Whilst the test concentrated on cleaners being in the building (due to them being in the office more frequently at present) there is a need to consider other contractors in the building at all other times.

- 4.3.9 The BS advised that he was aware that there was an element of data governance reflected in the contract with Pinner (who worked on the Riverside House 'mothballing' process) and he was aware that reference to GDPR was made in some of the recent contracts he had been involved in the letting of, but this was 'general' and did not necessarily reflect specific processes for coming into 'contact' with information as part of their attendance at Riverside House or other Council properties, although this may be covered by contractor management meetings as appropriate.

Risk

Staff from contractors may obtain and divulge data held at Council premises.

Recommendation

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.

- 4.3.10 The DSM highlighted that there has generally been less post being both sent and received. On the whole, the responsibilities of staff within the Corporate Support Team (CST) and the Copier Operative have remained the same and, as such, the staff were aware of their responsibilities with data being treated as was previously the case.
- 4.3.11 As staff are generally not in the office to obtain their incoming post, the documents are scanned and placed in specific network folders. The DSM advised that the folder structure appears to be working well, with the structure and the related security of the folders being built with ICT staff.
- 4.3.12 The CST Manager (CSTM) confirmed that, due to the nature of their work, the majority of staff within the CST were still office-based and continued with their normal responsibilities. One additional member of staff had also been co-opted into the team but was also aware of his responsibilities in terms of data security.
- 4.3.13 The CSTM suggested that there is the expectation that, if staff were to move department within the Council, their details would be updated on the intranet and their folder access would be amended appropriately so that they were able to obtain scanned documentation as required.
- 4.3.14 The Technical Support Analyst advised that, assuming that ICT were made aware of the change, they would ask the 'new' department for details of someone who has similar access requirements as the access to the post folders (amongst other things) is based on group access settings. The details provided for the new department would then be copied across for the staff member which would overwrite all of their existing settings.
- 4.3.15 The CSTM highlighted that, once scanned, documents are placed into the old post folders for each team. These are then reviewed on the first of each month with all post from the previous month being removed.

- 4.3.16 If staff need to obtain any printed materials, there is a print locker in place at Riverside House that staff can access without needing to enter the building. The BS advised that the lockers were only meant for certain types of documents (e.g. flyers) as opposed to anything that may contain personal / sensitive data which would be distributed separately. As such, it is considered that there is no issue in terms of data security with regards to the use of the lockers.
- 4.3.17 As part of the staff survey, specific questions were asked of staff as to whether they had received any post or requested printing whilst working from home and how they were ensuring data security in their new working environment (see 4.5 and Appendix B).

4.4 **Data Disposal**

- 4.4.1 The BS advised that there had been time to plan the clearance of relevant areas of Riverside House to allow staff to return to a COVID-safe office (not just mothballing of level four but clearance of other levels to allow staff to be moved), with a work process designed accordingly.
- 4.4.2 People were invited into Riverside House in groups to allow for the process to be supervised / controlled, with 'items' then classified as either staff needing it to be taken home (which had largely been undertaken when staff first started working from home), information (paperwork) that needed to be retained but not needed for working from home (either because there was no time to review it all or it needed to be retained), and then 'everything else'.
- 4.4.3 For items that needed to be retained but which were not being taken home, individual rooms / areas were allocated to each department, with some differentiation between what had previously been 'secured' (e.g. in locked cupboards) and what had been 'in the open'.
- 4.4.4 The BS advised that he had been on site along with the TBM each day to supervise the process and to discuss with staff what was required. There was an assumption that everyone had received their GDPR training but staff were told that, if in doubt, any paperwork should be put in the confidential waste bins for secure disposal.
- 4.4.5 Despite the staff 'briefings', the BS advised that it was surprising how much staff were still putting in the general waste and, following a 'near miss' (where it was identified that personal data had been placed in the general waste skip), staff were stopped from putting any waste in the skips. The BS and the TBM went through every general waste 'box' themselves which ensured that no personal data was placed in the general waste (and also allowed for greater levels of recycling).
- 4.4.6 The BS suggested that human error was the main issue and there were some repeat offenders who were very bad at disposing of their paperwork appropriately. The issue was reported to the Workforce Steering Group who advised the BS that he was able to flag any specific concerns with the relevant Head of Service.

- 4.4.7 The BS also highlighted that Pinner's were also briefed about putting any paperwork they found to one side so that it could be reviewed.
- 4.4.8 All paperwork from the office clearance was placed in the 'bike store' before being transferred to a shipping container for secure destruction.
- 4.4.9 The BS suggested that there were lessons to be learned from the process and he would have involved the IGM more in the process in hindsight. These 'lessons' should be taken on board, as staff still have to go through some of the documentation held where they didn't have time to review it all before it was moved to its current storage areas and there will also be further work required as and when the Council moves from Riverside House in the future.

Advisory

A 'lessons learned' report should be drawn up that can be referenced when any future building moves are undertaken.

- 4.4.10 A confidential waste bin is available at Riverside House for staff to use as needed. The DSM advised that the availability of the facility had not been well publicised, although reference to it had been made in response to a Rumour Mill question.
- 4.4.11 Due to the positioning of the bin (i.e. just inside the staff entrance), there was no real need for guidance around social distancing etc.
- 4.4.12 As part of the staff survey, staff were asked how they were destroying or disposing of data whilst working from home (see 4.5 and Appendix B).

4.5 Summary of Findings from the Staff Survey

- 4.5.1 162 responses were received to the survey issued via the intranet, with staff being asked a series of questions as highlighted in the previous sections. As suggested previously, a more detailed summary of the responses to the staff survey can be found at Appendix B. However, the 'issues' detailed in the following paragraphs need specific consideration.
- 4.5.2 In terms of training, almost 32% of the respondents did not feel that they had received appropriate training in relation to data security whilst working from home.
- 4.5.3 Supporting comments to this question and a follow-up question on what staff felt they needed training on suggested a number of general and more specific issues:
- 'General awareness'
 - The use of 'connected devices' (e.g. Amazon Alexa)
 - Confidential waste
 - Equipment security
 - General data security
 - 'I don't know what I don't know'.

The recommendation at 4.2.5 above should ensure that these 'issues' are resolved.

- 4.5.4 Two further specific training / guidance 'needs' where flagged, albeit, not directly relevant to data security:
- Mental health whilst working from home
 - MS Teams etiquette.
- 4.5.5 A similar question was asked in relation to staff awareness of policies and procedure documents that were relevant to their new / current working conditions. Approximately 39% of respondents answered that they were not aware of relevant documents. Again, the guidance produced in reference to the recommendation at 4.2.5 should make reference to any relevant policy / procedure documents.
- 4.5.6 A question on the receipt of communication relating to data-related issues was also asked. Over 52% of staff were not aware of any relevant communication received although supporting comments from those who were aware of the communications made reference to notices such as those referred to at 4.2.8 above.
- 4.5.7 Whilst not relevant to the question on communication, two responses also detailed security 'incidents' that had affected the individuals:
- A personal phone number had been used as a WDC number
 - A staff member's email address had been included in a 'rehousing' email which led to threats from neighbours
- As these are one-off incidents, it is not considered that there is a need for a specific recommendation. However, it was felt that there was a need to make reference to these issues so that management are aware that these had been flagged by staff.
- 4.5.8 A question was asked about current working conditions for staff working from home. Whilst responses were understandably varied, a number of those who were working in rooms that were not dedicated offices suggested that they are working on tables as opposed to office type desks (20) and three people were working in cramped spaces. Whilst this audit is concerned with information governance, there is an obvious impact on health and wellbeing from some of these working conditions which is felt to be worth highlighting.
- 4.5.9 A follow-up question was also asked as to whether anyone else used the 'office space'. Almost a third of respondents confirmed that others use this space and, whilst in hindsight the question could have been made clearer as to whether this was whilst the individual was working (e.g. someone else may use the lounge but not whilst the staff member was working there), and staff may well be taking precautions to ensure that data security is maintained, there is undoubtedly an information governance implication from working in shared spaces with non-WDC staff.

Risk

Staff may be working in unsuitable working conditions, both in terms of health and wellbeing and data security.

Recommendation

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.

- 4.5.10 One particular issue that the IGM flagged during the opening meeting for the audit was the prevalence of 'connected devices'. Questions were, therefore, asked as to whether staff had them in the work spaces and whether the listening facility was being disabled whilst working from home.
- 4.5.11 Only 28 respondents suggested that they had such a device in their work space and the majority of those suggested that they turned the listening facility off. However, comments in relation to other questions suggest that some staff were not aware that using one of these devices could have data security implications, so further (or reinforced) guidance (as recommended at 4.2.5 above) may be useful.
- 4.5.12 Another question asked staff how they were storing and securing the data they obtained. The comments were very varied due to the nature of the question but specific references were made in a number of cases in relation to the security of 'confidential data' (or that they didn't hold any such data).
- 4.5.13 However, as flagged by the BS, some staff appeared unaware of what constituted relevant personal / sensitive data when they visited RSH to clear their areas so there may be some false sense of security when staff talk about ensuring that 'confidential' data is secure.
- 4.5.14 There were also a number of responses where staff advised that they hold paper documents but did not specify whether these were secure. It could well be that they are maintaining security, but it could be part of a wider issue of staff not having the capacity to store data securely when working from home.
- 4.5.15 Methods of dealing with distractions to ensure that data was not inadvertently disclosed whilst working from home were also covered by a question in the survey. Specific examples were given to staff (i.e. sending emails to the wrong recipient and putting documents in with general waste) as these had been the subject of previous data breaches or near misses.
- 4.5.16 In a similar vein to other questions, some respondents made specific reference to separating confidential waste from other documents. One person also highlighted that they put their notebooks in the general waste. Again, there may be a need to flag that some 'notes' taken may contain personal data whilst not being formally classified as confidential.
- 4.5.17 Another response also hinted at a false sense of security in relation to emails. They highlighted that "they work on a work laptop, so can't email 'randoms'".

This obviously doesn't stop someone from picking the wrong email address from the auto-fill drop down lists so this may also need reinforcing in the guidance issued.

- 4.5.18 Again, there were also responses that suggested that working from home may not be suitable as a long term solution for all (e.g. hard to avoid distractions from others in the house, no means of disposing of data etc.). This was also raised in a subsequent question on screen positioning whereby a member of staff was unable to position their monitor such that others passing the property may be able to read what is on the monitor.
- 4.5.19 The use of personal equipment was also covered in the survey. Roughly 38% of respondents suggested that they had or were using personal devices for work and, whilst the majority of comments suggested that data security was not an issue, one specific response in relation to use of their personal phone went into quite some detail on the suitability of their device and the issue that they are dealing with:

I have to use my personal phone for photos due to my work phone a) not allowing me to store or send them to my work email. b) My data allowance is dangerously small. c) I would rather my work phone was used! I always send them to hsgem, then process / delete from my phone, and empty my trash which is very time consuming, limits my working process and I do not wish to have the kind of horrible insanitary photos I have to take on my personal device. Nobody else uses my phone however I find I am restricted because I won't use my own device to show family/friends photo's especially if I have used it for work that day. Please arrange for work phones to be able to be used for work photos and have enough data to do the job properly, I would hate to have this facility and then find it is too restrictive to do the job properly. In very poor properties I can take 30 plus photo's in initial visits. My data is all used and I can't send them anywhere.

- 4.5.20 Whilst this is only one specific responses, anecdotal evidence suggests that others may also be experiencing similar issues with the suitability of their devices.

Risk

Staff may not be able to deal with data securely.

Recommendation

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).

- 4.5.21 The final questions covered disposal of the data held. The issues flagged in the responses to these questions generally fell into the previously reported 'category' of staff potentially not knowing what may include personal data when referring to 'confidential' documents and others seemingly discarding 'notebooks' in general waste.

5 Conclusions

5.1 Following our review, in overall terms we are able to give a MODERATE degree of assurance that the systems and controls in place in respect of Information Governance are appropriate and are working effectively.

5.2 The assurance bands are shown below:

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

5.3 Issues that require further action were identified:

- There is a need for a staff guidance document in relation to various data security aspects highlighted within the report
- Staff from contractors attending Council offices may obtain access to data
- Current working conditions for some staff may not be suitable both in terms of health and wellbeing and information governance
- Work-issued devices may not be suitable for work performed by some staff to enable appropriate data security.

5.4 A further 'issue' was also identified where an advisory note has been reported. In these instances, no formal recommendations are warranted as there is no risk if the actions are not taken. If the changes are made, however, the existing control framework will be enhanced:

- A 'lessons learned' report in relation to the clearance and mothballing of parts of Riverside House would be useful for any future office moves.

6 Management Action

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

Richard Barr
Audit & Risk Manager

Action Plan

Internal Audit of Information Governance – March 2021

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.5	A guidance document, pulling together all issues identified, should be drawn up and distributed to all staff.	Staff may not be aware of data protection issues that impact their way of working.	Low	Information Governance Manager	Agreed. A guidance document will be drawn up and issued accordingly.	30 June 2021
4.3.9	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.	Staff from contractors may obtain and divulge data held at Council premises.	Low	SMT	Contract managers will be asked to review their contracts to ensure that the need for data security has been appropriately considered in each case.	30 September 2021
4.5.9	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.	Staff may be working in unsuitable working conditions, both in terms of health and wellbeing and data security.	Medium	SMT	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.	30 September 2021

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.20	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).	Staff may not be able to deal with data securely.	Medium	SMT	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.	30 September 2021

* Risk Ratings are defined as follows:

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

Summary of Responses to Staff Survey on Data Security



18 questions were included in the staff survey, with the first two just asking for the name and department of the respondent. 'Issues' raised or identified from the responses are recorded in section 4.5 of the main report.

Q3 asked respondents to describe their current working conditions. The 161 responses can be summarised into the following categories (NB the total does not equal 161 as some comments are included in more than one category and some responses were not relevant. Those who answered 'N/A' in the comments to this (and any other) question have been removed from the number of comments recorded):

Location	Number
Bedroom (including spare / box rooms)	54
Dedicated office / study	49
Lounge / living room	24
Dining room	18
'Open Plan' spaces	9
Kitchen	7
Other rooms at home (e.g. conservatory)	10
Riverside House (or other WDC offices)	5

A number of those who were working in rooms that were not dedicated offices suggested that they are working on tables as opposed to office type desks (20) and three people were working in cramped spaces.



A follow up question was also asked as to whether anyone else used the 'office space'.



4. Does anyone else use this 'space'?				
			Response Percent	Response Total
1	Yes		32.08%	51
2	No		67.92%	108
			answered	159
			skipped	3

As per the figures above, almost a third of respondents confirmed that others use this space. Whilst, in hindsight, the question could have been made clearer as to whether

this was whilst the individual was working (e.g. someone else may use the lounge but not whilst the staff member was working there), and staff may well be taking precautions to ensure that data security is maintained, there is undoubtedly an information governance implication from working in shared spaces with non-WDC staff.

One particular issue that the IGM flagged during the opening meeting was the prevalence of 'connected devices' (e.g. Amazon Alexa, Google smart hubs etc.). Questions were, therefore, asked as to whether staff had them in the work spaces and whether the listening facility was being disabled whilst working from home:

5. Are there any 'casual listening devices' (e.g. Amazon Alexa) in this 'space'?				
			Response Percent	Response Total
1	Yes		17.39%	28
2	No		82.61%	133
			answered	161
			skipped	1



6. If so, do you turn off the listening facility while working?				
			Response Percent	Response Total
1	Yes		31.88%	22
2	No		68.12%	47
			answered	69
			skipped	93

(NB there is a clear anomaly between the numbers who said that they had a device (28) and the total number who responded to the follow-up question (69) – it is assumed that the majority of the 'no' answers were respondents who did not had a device but chose to answer no as opposed to skipping the question).

From the figures, it appears that the majority of respondents who have a device turn off the listening facility, but comments in relation to other questions suggest that some staff were not aware that using one of these devices could have data security implications, so guidance may be useful.

The next four questions covered training, guidance and communications:

7. Have you had appropriate training/guidance on how to deal with data security whilst working from home?

			Response Percent	Response Total
1	Yes		68.15%	107
2	No		31.85%	50
			answered	157
			skipped	5

62 supporting comments were provided for question 7. In summary, these fell into a number of general categories:

Theme	Number
Common Sense	7
Intranet / Emails / Guidance / Discussions	20
'General' training	12
'Prior / Non-WDC' training	3
Same as being at Riverside House	7
None / can't remember	6

Two specific comments to note (which may not relate directly to the question asked, but were provided in the comments for this section) were:

- 'I wasn't aware that Alexa could impact security'; and
- 'No **proactive** training received'



A follow up question (Q8) was asked – 'If not, what do you believe you need training/guidance on?'. This elicited 38 responses, although a number were not relevant (e.g. related to the previous comments on Q7 as opposed to identifying training needs). Again the relevant responses fell into a number of general categories:

Theme	Number
General awareness	5
Connected devices	4
Confidential waste	1
Equipment security	1
Data security	5
'Don't know what I don't know'	5

Two further specific training / guidance 'needs' were flagged, albeit, not directly relevant to data security:

- Mental health whilst working from home
- MS Teams etiquette

9. Are you aware of any relevant policies/procedure documents relevant to your new/current working conditions?



			Response Percent	Response Total
1	Yes		61.25%	98
2	No		38.75%	62
			answered	160
			skipped	2

26 supporting comments were made which referenced a number of specific 'policies' and other guidance (more relevant to the previous questions):

Theme	Number
Data Protection 'Act'	1
Display Screen Equipment (DSE)	2
As at Riverside House	5
GDPR	2
WDC Data Security Policy	1
ICT Security Policy	1
'Home Working Essentials' article	5
Meta notices	1
Intranet / Email guidance etc.	10
COVID FAQs	1

One comment suggested that 'there should be a meta compliance test'.

10. Have you received or are you aware of any communications relating to data-related issues that have occurred due to home working/current working conditions?

			Response Percent	Response Total
1	Yes		47.83%	77
2	No		52.17%	84
			answered	161
			skipped	1



33 supporting comments were made which referenced a number of specific issues that had been communicated or general comments about where the notice had come from:

Theme	Number
Topics	
Auto-fill / email trails	11
Screen security	2
Home printing	2
Shredding / confidential waste	2
Password security	1
Source	
Meta communications	2
Intranet notices	7
Emails	2

Two responses also detailed security 'incidents' that had affected the individuals:

- A personal phone number had been used as a WDC number
- A staff member's email address had been included in a 'rehousing' email which led to threats from neighbours

The next two questions asked about the receipt of post and printing:

11. Have you received any post/requested printing whilst working from home?			Response Percent	Response Total
1	Yes		41.61%	67
2	No		58.39%	94
			answered	161
			skipped	1

Where staff had answered yes to Q11, Q12 asked how this had been obtained. 70 responses were provided which fell into a number of general categories:

Theme	Number
Posted home	12
Visit RSH / Team members at RSH deal with it on their behalf	37
Of the above – specific mention of use of Print Locker	10
Visit to another WDC location	5
Outgoing / incoming mail folders on network	7
Via CST / Mike Pratley	14
Email	6
Own approved printer	1

Q13 asked 'How is the data you obtain (through any means) stored/secured whilst working from home (e.g. from others in the house etc.)?'. The 149 comments were very varied due to the nature of the question but, again, they can be largely summarised into one or more themes:

Theme	Number
Electronic	100
Work equipment	36
Devices / screens locked or shut down	36
Only person in the house (at least during working hours)	11
Locked / closed office	6
Locked desk	6

Theme	Number
Various 'folders' / storage areas (not specified whether locked / securely held)	30
'Own part of office'	3
Note books / paper documents (not specified whether held securely)	10
Clear desk	2
Unspecific 'securely held'	3
'Unsecure / unable to secure'	2
No data(!)	1

Five respondents made specific reference to the security of 'confidential data' (or that they didn't hold any). However, as the Building Surveyor, some staff appeared unaware of what constituted relevant personal / sensitive data when they visited RSH to clear their areas so there may be some false sense of security when staff talk about ensuring confidential data is secure. It is also slightly alarming that one person felt that they didn't deal with any data!

As can be seen from the above table, there are also a number of people who appear to hold paper documents that did not specify whether these were secure. It could well be that they are maintaining security, but it could be part of a wider issue of staff not having the capacity to store data securely when working from home.

The next question (Q14) covered dealing with distractions to ensure that data was not inadvertently disclosed whilst working from home. Specific examples were given (i.e. sending emails to the wrong recipient and putting documents in with general waste) as these had been the subject of breaches or near misses. 140 responses were provided to this question, with some covering one of the examples, some covered both and some gave more general comments (not all of which were applicable!).

Numbers for those who said that they hadn't got any paper records were discounted, as the question was around dealing with distractions as opposed to whether there was anything that could 'go wrong' if they were distracted. Some also highlighted that they had the same amount / less distraction than they would while working at RSH or they would deal with distractions in the same way that they would whilst working in the office.

The other responses can be summarised as:

Theme	Number
No distractions (e.g. work away from anyone else at home)	26
Manage distractions (e.g. stop working)	6
Use a personal shredder / incinerator	26
Emails checked / auto-fill turned off	24

Theme	Number
Not disposing of work 'waste' at home / use of confidential waste bin at RSH	11
Generally 'being careful'	10
Had actually sent emails to the wrong person	3

In a similar vein to other questions, some respondents made specific reference to separating confidential waste from other documents. One person also highlighted that they put their notebooks in the general waste. Again, there may be a need to flag that some 'notes' taken may contain personal data whilst not being formally classified as confidential.



Another response also hinted at a false sense of security in relation to emails. They highlighted that 'they work on a work laptop, so can't email 'randoms''. This obviously doesn't stop someone from picking the wrong email address from the auto-fill drop down lists.

Again, there were also responses that suggested that working from home may not be suitable as a long term solution for all (e.g. hard to avoid distractions from others in the house, no means of disposing of data etc.)

Q15 covered screen positioning at home, to ensure that data on the screens could not be overlooked by people passing the property. Only four of the 158 responses suggest that there was a potential that data on their screens could be seen by people from outside of their house, although one may be discounted as they suggested that this was 'mitigated' (door closed whilst working).

One again specifically flagged the suitability of their homeworking environment in this regard ('Due to the size of my office at home I have no choice on where it (the screen) has to go. Visible from the footpath and road')

The next questions covered the use of personal equipment and whether there was any data stored on it or if others had access to it:

16. Do you use any personal equipment for work (e.g. personal laptop/iPad etc.)?				
			Response Percent	Response Total
1	Yes		38.13%	61
2	No		61.88%	99
			answered	160
			skipped	2

64 responses were provided to the follow-up question (Q17) regarding storage and access. Again, some responses cover more than one topic and can be summarised as:

Theme	Number
No data stored	25
Nobody else has access	17
Only used for Teams / Jabber / Outlook etc.	22
'No' (general answer, could be covering one or both aspects of the question)	15
Protected by password / software	3
Work-related photos / phone numbers held on device due to capacity / capability etc. of work-provided equipment	4
Others have access to device	3
'Other storage' (videos on SD card)	1

One of the respondents who uses their personal phone for photos gave an in-depth answer to the issues they were dealing with:

I have to use my personal phone for photos due to my work phone a) not allowing me to store or send them to my work email. b) My data allowance is dangerously small. c) I would rather my work phone was used! I always send them to hsgem, then process / delete from my phone, and empty my trash which is very time consuming, limits my working process and I do not wish to have the kind of horrible insanitary photos I have to take on my personal device. Nobody else uses my phone however I find I am restricted because I won't use my own device to show family/friends photo's especially if I have used it for work that day. Please arrange for work phones to be able to be used for work photos and have enough data to do the job properly, I would hate to have this facility and then find it is too restrictive to do the job properly. In very poor properties I can take 30 plus photo's in initial visits. My data is all used and I can't send them anywhere. Thank you

The final question (Q18) covered data disposal and destruction. A range of answers were given, with some respondents also covering this as part of Q14 when commenting on their methods of ensuring that data wasn't disclosed inadvertently due to distractions (specifically around access to shredders / incinerators etc.)

The 139 answers to Q18 can be summarised as follows (NB a number of responses such as 'do not have any / no paperwork etc. were not counted):

Theme	Number
All held electronically	33
Shredder / Incinerator / other 'unspecified' destruction methods	49
'Deleted'	12

Theme	Number
Brought to RSH / waiting to be able to bring to office	23
Not destroying whilst WFH	6
'Only' notebooks	3
Bin (household waste)	2
'Confidential' 'ripped up, not confidential in recycling	1

Similar issues to previous questions were highlighted in relation to disposal through unsecure means and the 'confidential' aspects of data.