POLICY REVIEW COMMITTEE

SCRUTINY REVIEW OF DATA SECURITY

CONTENTS

Appendices:
Appendix A – Question List

Timeline:	1 October 2020	Policy Review Committee (P/20/10)
	11 November 2020	Executive (EX/20/69)

1. Foreword

1.1 The Policy Review Committee would like to present their review into the issue of data security within the data management processes of Hertsmere Borough Council.

1.2 We undertook this review because Committee Members sought assurance that security risks had been mitigated now that data was stored on the Cloud and that data security was sufficiently robust.

1.3 We would like to thank the following Council Officers who helped us during the course of our work:

- Matthew Bunyon – Head of Finance and Business Services
- John Robinson – Information & Digital Services Manager
- Dave Casling – Infrastructure and technical Security Team Leader
- Harvey Patterson – Head of Legal & Democratic Services
- Shane Kenny – Information and Data Protection Officer.

Scrutiny Review carried out by:

Cllr Briski
Lead Member

Cllr Carter

Cllr Mortimer

Cllr Myers

2. Summary

2.1 We have been satisfied, via our detailed sessions with key Officers and through our review of the Council's data management documentation, that Hertsmere Council is handling personal data in a secure way and is complying with the relevant legislation, including in relation to commercial agreements with third-parties.

2.2 Our enquiries identified no system-based errors and that measures are in place to manage human errors. Paper-based data security appears to be good and the processes in place appear adequate.

2.3 Processes for dealing with data breaches is good, with regular audits and the Public Services Network Compliance Certificate has been achieved. Systems are locked as much as is reasonable eg USB ports on printers are locked and staff cannot set up personal printers but we do not think it necessary extend such measures to camera phones and the like.

2.4 The cloud contract and support desk is good and will allow the Council's ICT provision to grow as required, eg for flexible working, and will make

data management easier, eg auto-deletes can be enabled with the legally-compliant retention limits/thresholds.

2.5 In summary, the Council has taken a measured approach with its ICT security and our recommendations seek to support that approach.

2.6 The Executive is asked to consider our recommendations and the reasons behind them and to take the necessary steps to implement them.

3. Recommendations

The Policy Review Committee recommend to the Executive:

3.1 **consider whether some departments should have predictive text removed to prevent communications being sent to the wrong person, given that the Data Breach Log shows this to be a common-place error.** *[see para 5.9]*

3.2 **that the Data Breach Log be reported annually to Operations Review Committee and the Log must identify where a breach is due to the same task/department/person (person's name to be anonymised)** *[see para 5.10]* **and that the Log include a separate section for data breaches that were not due the Council but by external parties, or where it is unclear how the breach occurred only that it had occurred.** *[see para 5.7]*

3.3 **that where a person/department mis-addresses an e-communication three times, then predictive text should be disabled for them.** *[see para 5.9*

3.4 **that breaches of printed/hardcopy data should be included in the Data Breach Log** *[see paras 5.2, 5.10]*

3.5 **that the Council should make its processes paperless wherever possible, eg introduce personal accounts for residents to log into to manage payments etc, because this will reduce communication breaches and help to tackle climate change.** *[see para 5.23]*

3.6 **that the Council's achievement of the Public Service Network Compliance Certificate should be publicised more prominently, eg on the Council website, so that residents are reassured about data security.** *[see paras 5.3, 5.14, 5.16]*

3.7 **that a Retention Schedule should be adopted that meets the requirements of the General Data Protection Regulation and draws upon the Public Records Office model.** *[see paras 5.24, 5.26]*

3.8 **that mandatory training on data security should be provided to all Councillors.** *[see para 5.5]*

3.9 **that an iPad Customer Workshop should be held with a mix of high-intensity and low-intensity users, IDS staff and the Community Safety and Performance Portfolioholder to ascertain the essential level of security locks that must be enabled on the Council iPad, as currently they were completely locked-down and hindering Councillors from easily carrying out basic tasks, eg report writing.** *[see para 5.6]*

4. Objective of the Scrutiny Review

4.1 The objective of the Review was to ascertain the status of the following:

(i) The Data Management processes of this Council.
(ii) How security risks had been mitigated now that data was stored on the Cloud?
(iii) Was data security sufficiently robust to give residents assurance that their data was secure?
(iv) What measures are in place to prevent the unauthorised access of sensitive data?
(v) How the movement of sensitive data is monitored, especially when transferred out of internal systems?
(vi) Whether the Council's policy relating to data protection is compliant with all relevant legislation?

5. Background

5.1 To meet our objective we reviewed the Council's data management policies and spoke with the key Hertsmere Council Officers who had responsibility for dealing with data security. A list of the questions we asked is attached at Appendix A.

STATUS OF THE COUNCIL's DATA SECURITY POLI CIES and PROCESSES

5.2 We looked at the IDS Facilities Usage policy and were told that it covered all forms of information including hardcopy. Its purpose was to prevent data loss as well as protect staff and data. We ascertained from Officers that it was being reviewed and a significant change to it was the introduction of a single complex password to obviate the necessity of regularly updating passwords. Additionally a number of audits, including a cyber-security audit, had been carried out in 2019 and any recommendations arising from those audits would be incorporated in the updated IDS policy.

5.3 Officers also informed us of that the Council always obtained the annual Public Services Network Compliance Certificate to allow it to connect to

central government networks – and that this Certificate could only be obtained by passing various audits and checks. So this was another assurance of the robustness of Council's data management systems. We considered this external measure of the robustness of the Council's systems reassuring and that it should accordingly be more widely publicised. **[see Recommendation 3.6]**

5.4 It seemed to us that the Council has very good policies and approaches in place to ensure good data security and overall we were pleased with the policies that are in place.

HOW ARE BREACHES ADDRESSED

5.5 Officers informed us of the "Security Breach Procedure" policy which covered different types of breach. Staff were required to report any breaches to the IDS Service Support Desk, which would then be referred to the Information Officer, who had 72 hours in which to determine whether or not the breach was serious and must be reported to the Information Commission Officer. There was a mandatory data security training module for all staff via the Council's online training programme, "The Learning Zone" and staff's test results and performance were recorded as part of the training process. We suggested that this training should be undertaken annually by staff and Councillors and monitored to ensure it had been undertaken **[see Recommendation 3.8]**.

5.6 With regard to training we were aware of fellow Councillors were interested in using their iPads in an as security-conscious manner as possible. Councillors had varied purposes for using their Council iPads and also different levels of expertise, so an accordingly tailored training session would be useful to them. We suggest a Workshop should be held with a mix of high-intensity and low-intensity users, IDS staff and the Community Safety and Performance Portfolioholder to ascertain the essential level of security locks that must be enabled on the Council iPad, as currently they were completely locked-down and hindering Councillors from easily carrying out basic tasks, eg report writing. **[see Recommendation 3.9]**.

5.7 We additionally looked at the Log of Recent Breaches, and Officers also informed us of the breach process. We noted there had been very few data breaches and they had not been serious in nature, eg the inadvertent use of drop-down menus on software programs, including email]. Within local government, core services were now almost all automated and there were very few manual systems still in operation with the attendant data security risks posed by such systems. Other than personal information, the only other recent data breach had been the circulation of a "Not for Publication" Audit Committee report in the public domain, but this was not proven to be a breach by the Council as other external organisations had that same data. We suggest that the Log could usefully have a separate section for breaches of data that were not due the Council but by external

parties, or where it is unclear where the breach occurred only that it had occurred. **[see Recommendation 3.2]**.

5.8 Officers highlighted that deliberate data breaches could result in criminal sanctions under various statutory provisions such as the Misuse of Computers Act 1990. Additionally, any breaches by Officers were dealt with under the Council's disciplinary code and in the case of breaches by Members these were dealt with under the Standards regime.

5.9 In terms of prevention and resolution, Officers always sought to introduce measures to prevent a re-occurrence of the breach discussing the breach and preventative measures to be put in place with the employee's line manager and the employee. Where it was not possible to take preventative measures, eg if an individual acted deliberately, then a person may be placed on "Garden Leave" until the matter was resolved. We seggest where errors are due to predictive text, options to disable it should be considered. **[see Recommendations 3.1 and 3.3].**

5.10 The Breach log showed us that there had only been six non-serious breaches in a seven month period. The Council used electronic systems to generate information and communicate with residents. Consequently, there was an inherent risk of a breach of the data stored and transmitted by these systems. However, the fact that members of staff were coming forward whenever there may have been a data breach indicated that there had not been any core system failures and that data breaches were more likely to be a result of human error. Given that the IDS Facilities Usage policy covered hardcopy data we suggest that the Log should cover breaches of printed/hardcopy data. **[see Recommendation 3.4]**. We also considered a useful activity for Operations Review Committee to get an annual monitoring report on the Data Breach Log setting out the breaches of the past year and identifying whether breaches were due to the same task/department/person. However the name of the person should be anonymised (eg just state Person X) on data protection grounds and so as not to discourage whistle-blowing. **[see Recommendation 3.2]**.

TESTING THE SYSTEMS

5.11 We were concerned as to what was in place to prevent someone with access to the Council's networks and systems from transferring sensitive information to a flash drive or personal email account.

5.12 We were advised that all USB ports on Council computers were blocked making flash drives inoperable. Access was given by exception to some Officers to use Hertsmere BC encrypted flash drives in Council computers and devices where their job required it. Anything copied from a Council computer onto a flash drive would be recorded in the Council's Data Loss Prevention (DLP) system. Emails sent using the Council's email system were encrypted and there was a block on personal email addresses such

as Yahoo and Hotmail, and file upload sites such as Dropbox. Moreover the Council had insurance for any criminal activity regarding the use of flash drives and Council computer equipment.

5.13 In terms of monitoring access to confidential information, a log of printer activity was recorded using a Security Information Event Management System and an alert would be raised when, say, a new user was added to a group. However, given the volume of printing carried out using Council devices, only when there was a specific request would an investigation be carried out in relation to printed documents. The introduction of Microsoft 365 Enterprise would give greater control over documentation, and in fact an inclusion of sensitivity levels in the Information Security Policy would support an application to the Executive for the renewal of the Microsoft Enterprise agreement and the introduction of Microsoft 365 Enterprise.

5.14 In response to our queries, we were told that the default position was for data to be encrypted, including data that was in transit, eg emails. Data that was "at rest", such as that in the virtual environment, need not be encrypted as the physical security of the information, including servers, was of greater relevance. The Government had previously required the use of encrypted email services such as Egress, it was now of the view that the Internet was sufficiently secure if emails were encrypted in transit. This change had been reflected in the Council's Public Services Network. **[see Recommendation 3.6]**.

5.15 As for access to the Council's servers, a log was kept of who had access and only a limited number of persons, including contractors, had access to the actual servers. With regard to paper files, many had now been scanned and were in electronic form. Consequently, there was less personal information kept in paper format but there was provision within the Council for the disposal of confidential paper waste. There were also Banking Industry Standard card security systems in place to protect credit and debit card transactions conducted using the Council's payment systems.

5.16 We were enquired whether any devices connected to the Council's network running outdated software which no longer supports security updates. We were told that no devices in the Council's network ran outdated software as to do so would be contrary the Council's Public Services Network Compliance Certificate. **[see Recommendation 3.6.]**.

5.17 We checked the status of the anti-virus software used by the Council and if there were options to improve it. Officers advised us that the Council used McAfee anti-virus software which served the needs of the Council and had the advantage of being centrally managed and, therefore, automatically updated with regular reports and logs being produced.

5.18 In terms of printer vulnerabilities, we were told that this would be detected during a scan of the Council's systems and software updates and

patches and that the function to print from the USB ports on the Canon printers has not been enabled.

5.19 We enquired about security risks in relation to the Wi-Fi networks. Officers advised us that of the four Wi-Fi networks, only one connected to the Council's network and only devices that were logged on to the Council's LAN with the appropriate certificate had access to the Council's network and only IDS staff knew the password to connect to the Council's network.

CLOUD and THIRD-PARTY SECURITY

5.20 We were advised that the Council's Strategy aligned with the Government's recommendation of Cloud First. Accordingly, when a system came up for renewal, and there was a business case, a cloud-hosted solution would be sought thereby moving systems off-site e.g. the new CRM system which would be hosted within the supplier's cloud environment. It was anticipated that, over the next five years, the Council would develop a hybrid cloud infrastructure.

5.21 The Council's payroll system had recently been moved to the supplier's hosted site, one of the drivers for this being partnership working with Hertfordshire Building Control Company. In addition, HR were looking to upgrade its Attendance & Timing system and, in so doing, moving this to the supplier's cloud. The main system being trialled was the Revenue & Benefits system which was being hosted on a public cloud using supplier provided software.

5.22 Regarding clauses contained within commercial contracts, we were informed that issues of data protection and compliance would form part of any contractual terms and conditions or any variation thereof of existing contracts. Furthermore, since the introduction of the General Data Protection Regulation (GDPR), any new contracts that the Council might enter into would require suppliers to have a GDPR policy in place and existing contracts were being reviewed to ensure that they had the relevant GDPR provisions in place. As for the sharing of sensitive information with contractors and suppliers, Officers stated that most of the Council's systems contained confidential and/or sensitive information and that contractors and suppliers were under a legal obligation to comply with statutory obligations regarding such information.

AREAS FOR IMPROVEMENT

5.23 We were advised that moving existing systems to cloud-based systems had implications for data retention as there was a cost associated with the amount of data retained. On the other hand moving to a cloud-based system and the implementation of a GDPR module would automate the process of deleting old data, eg the Revenue & Benefits system would be doing exactly that. Deletion of data could become an annual process whereby the last year for which data was held would be automatically

deleted at the start of each year. Such deletion would have to account for any legal requirements to retain some data for specified periods, eg financial data and other data that must be kept indefinitely. In line with this approach, we felt a further area for improvement would be for the Council to make its processes paperless wherever possible, eg introduce personal accounts for residents to log into to manage payments etc, because this would reduce communication breaches and help to tackle climate change. **[see Recommendation 3.5]**.

5.24 Following the appointment of an Information Officer, issues of data retention were now being addressed and a Data Retention policy would be produced, which would improve data management processes in the Council. **[see Recommendation 3.7**].

5.25 Also to manage the duplication of data on Council systems, file analysis software ("Active Navigation") was being installed which would search shared drives for duplicated data.

5.26 Article 30 of the GDPR requires a Register of Retention Schedules to be maintained – because a requirement of data protection is to only retain personal information for as long its use is a justifiable necessity. The Council was updating its Data Protection and GDPR policies and compiling a Register of Retention Schedules, in doing so it would use the Public Records Office's model retention schedules as a guide. We suggested that we should draw upon any best practice provided by the Public Records Office. **[see Recommendation 3.7**].

6. Conclusion

6.1 We have been satisfied, via our detailed sessions with key Officers and through reviewing of data management documentation, that Hertsmere Council is handling personal data in a secure way and in doing so is complying with the relevant legislation, including in relation to commercial agreements with third-parties.

6.2 The Policy Review Committee will review the effectiveness of the response to its recommendations at its meeting on 21 January 2020.

Report produced by
Councillors Briski [Lead Member], Carter, Mortimer and Myers
on behalf of Policy Review Committee, August 2020

APPENDIX A – QUESTION LIST

QUESTIONS

1. Why has the Council's Information Security Policy not been reviewed since April 2017? This is particularly concerning given that new GDPR requirements have taken effect since the last review was due.
2. Have any data breaches occurred since the last review and what lessons have been learned? Please provide details of any incidents where any attempt was made to compromise sensitive information.
3. How are data breaches identified and what procedures are in place to respond to them?
4. What protection is in place to prevent someone with access to the Council's networks and systems from transferring sensitive information to a flash drive or personal email account?
5. When a confidential document moves out of the Council's systems, what monitoring is in place to identify the individual who did that?
6. Please provide details of the kind of information that is stored on-site and on the cloud. What is the Council's plan for moving forward with cloud-based solutions and what protection will be in place as we continue this journey?
7. Is sensitive information usually encrypted or stored in plain-text? Please provide separate answers for information stored on the cloud and information stored on-site, as well as the different levels of confidentiality the Council has in place.
8. Are any devices connected to the Council's network running outdated software which no longer supports security updates? For example, do any computers connected to the network still use Windows XP?
9. What anti-virus software is used by the Council and is it up to date? Can any recommendations for improved protection be made?
10. What mandatory information security awareness training is required from staff with access to the Council's network?
11. Are there possible vulnerabilities in the printer network?
12. What protection is in place to prevent a device connected to the Council's systems from acting maliciously? What measures are in place to ensure only authorised devices can connect to the network?
13. Could you explain the difference between the Council's different WiFi networks and the measures in place to prevent unauthorised access to the secure network?
14. What clauses are contained within commercial contracts with third party suppliers that the Council works with to ensure protection of sensitive information shared with them?

15. Who has overall control of the Council's IT systems? Should protection be in place to ensure that no single user can alter logs of people that have accessed sensitive information without approval from elected members?
16. Finally, can any further recommendations be provided to assure residents that the Council is adequately protecting their sensitive data? Is there something we should be doing that we're not doing already?