This Report will be made public on 4 July 2023

Report Number **C/23/12**

To:	**Cabinet**
Date:	**12 July 2023**
Status:	**Non key**
Responsible Officer:	**Amandeep Khroud, Assistant Director of Governance, Law and Service Delivery**
Cabinet Member:	**Councillor Fuller, Cabinet Member for Resident Engagement and Accountability**

SUBJECT: **INFORMATION GOVERNANCE – DATA BREACHES**

SUMMARY: At the meeting of the Finance and Performance Scrutiny Sub-Committee held on 7 March 2023, the Sub-Committee recommended that a report be brought before Cabinet to provide detail around the reported data breaches, and the measures put in place in order to prevent further breaches going forward. On 24 March 2023, Cabinet endorsed this recommendation.

REASONS FOR RECOMMENDATIONS:
Cabinet are asked to note the report in order to offer reassurance that the authority is taking measures to reduce the number of data breaches.

RECOMMENDATIONS:

1. **To receive and note report C/23/12.**

1. BACKGROUND

1.1 On 7 March 2023, the Key Performance Indicators for the third quarter of 2022/23 were reported to the Finance and Performance Scrutiny Sub-Committee. The Sub-Committee raised concerns around the reporting of data breaches.

1.2 The relevant performance figures, as well as the more recent figures for the fourth quarter and end-of-year position commentary, are shown in the table below:

Description	Q1 Actual 2022-23	Q2 Actual 2022-23	Q3 Actual 2022-23	Q4 Actual 2022-23	Target	2021-22 Comparison	2022-23 Summary	Target Met
All Subject Access Request responses to be provided within the statutory period (1 calendar month or lawful extension).	70.59% 12/17	66.67% 6/9	77.78% 7/9	61.54% 8/13	90% (Monthly)	28.95% (Average) 11/38	68.75% (Average) 33/59	X

1.3 The number of subject access requests (SARs) responded to over 2021/22 has shown significant improvement when compared with the previous financial year.

1.4 The resignation of one Case Officer and the subsequent appointment of another Case Officer into the Information Governance Specialist's role has had an impact on request turnaround times from Q3 onwards, particularly in the month of November. A new Case Officer was appointed at the end of November 2022 and this additional resource will help to ensure future performance will continue to improve to the required standard.

Description	Q1 Actual 2022-23	Q2 Actual 2022-23	Q3 Actual 2022-23	Q4 Actual 2022-23	Target	2021-22 Comparison	2022-23 Summary	Target Met
Percentage of data breaches assessed within 72 hours to decide if it is reportable to the ICO.	77% 10/13	70% 7/10	46% 6/13	67% 10/15	100% (Monthly)	100% (Average) 15/15	65% (Average) 33/51	X

Description	Q1 Actual 2022-23	Q2 Actual 2022-23	Q3 Actual 2022-23	Q4 Actual 2022-23	Target	2021-22 Comparison	2022-23 Summary	Target Met
Percentage of reportable data breaches that were submitted to the ICO within 72 hours.	n/a (no major breaches)	50% 1/2	0% 0/1	0% 0/1	100% (Monthly)	100% (Average) 4/4	25% (Average) 1/4	X

1.5 During this financial year, a new Specialist has been appointed from the Case Management team. They have been providing both resource and training to assist with improving overall resilience within Case Management. Furthermore, general InfGov training is ongoing with several members of Case Management (Corporate Services) involved, which will enable the Specialist to focus on work within their own queue, as they are currently providing ongoing resilience to the Case Management team whilst a new case officer is training.

1.6 Over the 2022/23 financial year, the new Specialist has been working with the Case Management Team Leader and Case Management Lead to bring more awareness to staff on what data breaches are and the importance of reporting them. This was in response to the discovery of several unreported breaches, which officers failed to report as they didn't recognise them as such. More training and education has been pushed through, and this has led to an increase in the amount of reports that are being reported.

1.7 In 2022/23, the information governance team have been notified of 51 breaches, four of which met the threshold to report to the ICO. A full breakdown of all reported breaches is shown at Appendix 1.

1.8 Whilst there has been an increase in these breaches being reported, these haven't been meeting the target for them to be assessed within 72 hours, over the 2022/23 financial year. This is largely down to service areas and individual officers not reporting them to the Information Governance Team promptly, with some still not being reported at all, or from the report being delayed through using the incorrect channels. This directly impacts the KPI for reports made to the Information Commissioner's Office (ICO) within 72 hours, as the report is sometimes only made to the Information Governance Team once 72 has already passed. As the number of breaches having to be reported is so low, missing the target for one of these drastically will often affect the KPI by 100%.

1.9 Most breaches that are occurring are minor, and are occurring through human error. This is usually through an officer accidentally entering the wrong contact to send emails to. Something else that seems to be occurring is where previously an officer has amended the contact address on the Council tax system, and general correspondence is subsequently sent to the incorrect address. In each instance here, the officer's line manager had a one to one meeting with them; explaining what they did wrong, how to avoid it in future and exactly why it's so important. Line managers will then usually hold a team meeting where they discuss how to avoid data breaches through their specific roles.

1.10 As a response to officers sending emails to the wrong recipient, a warning was added to Outlook earlier in the year which alerts officers if they are sending an email to anyone outside of the council domain. However, many emails are sent through the Salesforce system, and this safeguard cannot be applied within the system.

1.11 Officers will make small errors in their day-to-day work, and no amount of training will ever eliminate the potential for human error. The team have fairly recently been pushing data breach awareness amongst all staff, it would seem that the increase in cases is simply due to the breaches being recognised and reported; rather than being dismissed as an easy mistake. If we were receiving numbers of breach reports that were as low as previously, this is would be of greater concern.

1.12 Although there is more awareness within the Council now, there is still some work to be done with staff so that they recognise the urgency of the situation, to enable cases to be assessed within the statutory 72 hours. The Specialist has started to arrange additional training that will be supplied to individual teams during their monthly meetings. A training session for all management has been arranged to take place in October 2023. Further to this, we are looking to include additional education for all colleagues during a segment of a future staff briefing meeting.

1.13 The Specialist has found that most breaches occur when officers accidentally enter and select the incorrect email address or postal address when sending correspondence to a resident. The issues have continued to be raised with managers, and council-wide emails sent out to reiterate that all Council officers hold responsibility for assisting the Information Governance Team with investigating data breaches. It is our aim to make breach identifying and reporting second nature to officers, and not something to feel concerned about. Breaches will happen for as long as humans are there to make human errors, and that it's important that the instances are logged internally when it does occur. In the odd event where a breach occurs through other means, these are used to fine tune the general training provided and to streamline processes; to try to prevent them occurring again.

1.14 Currently, every member of staff is required to undertake annual GDPR e-learning training, and pass a test to demonstrate that they have understood the material. At present, 15% of staff have not recently carried out the GDPR training. This can be for reasons such as officers being on maternity leave or long-term sick leave. The new e-learning system enables managers to check officer progress against e-learning and it is the responsibility of managers to ensure that officers reporting to them complete the required e-learning training.

1.15 In addition, in December 2022 the Case Management Lead (Corporate Services) provided some additional training to the Customer Services Team. Officer training will be ongoing in the form of a presentation and Q&A session from the Information Governance Specialist. The training will cover how to spot a data breach, the importance of speed, how to report them and what the implications for the council may be. In addition, a more targeted approach will be taken to training. This involves identifying those teams with a higher rate of data breaches, using the new reporting features on Salesforce and raising awareness with those services with further education from the Specialist.

1.16 The main concern is the delay between officers becoming aware of a breach, and it actually being reported to the Information Governance team. This is the main factor with cases that aren't assessed within 72 hours of the council becoming aware of the breach, and subsequently being reported to the ICO within 72 hours (if needed). Each time this happens, the Information Governance Specialist will discuss this with the officer's line manager to ask that the sense of urgency is conveyed. This is reiterated to service area leaders when breaches are being investigated. This was included in a council-wide email, and subsequent reminder of the reporting process via SalesForce.

1.17 There have been several Council-wide 'reminder' emails from Information Governance management and senior colleagues over this period (and before) surrounding the importance of reporting data breaches, which has then resulted in breaches being reported more frequently. There is certainly more awareness surrounding them, which is positive. The team are working to make the thought of discussing potential data breaches less daunting, so that officers are confident and comfortable enough to report them. There has been a clear increase in data breach related calls and queries being sent to the specialist. Encouraging the comfortable discussion of these is vital in ensuring that they are reported as quickly as possible. This may also be a factor in the increase in reports being made.

1.18 The Specialist has begun working on several report features within the SalesForce CRM system used for cases – this should enable us to be able to run instant reports that will flag any areas and directorates within the Council who are frequently responsible for late breach reports or for failing to recognise them. Focused training can then be offered to these teams. We are also starting to record 'near misses' where there was the potential for a breach to occur, so that they can be used as opportunities to learn from. An example of the new report features can be seen at Appendix 2 to this report.

1.19 Overall, Information Governance is working in the most collaborative, organised, and effective way that it ever has, despite the loss of vital resource from the Case Management Team. Given time, the Case Management Team will be more knowledgeable, self-sufficient, and resilient, which in turn will enable the Specialist to focus on their own workload fully. As awareness continues to spread through the Council, as will staff's knowledge surrounding data breach reporting. We expect to see both an increase in reports and an increase in willingness from colleagues, which in turn will lead to KPI targets being met.

1.20 It should be noted that the information governance team are a high profile team within the organisation who face exceptional scrutiny and high work pressures, and cases are becoming increasingly complex. There is a tight labour market in terms of the information governance skillset and this presents a risk to the council.

1.21 Elected Members also have a responsibility in reporting data breaches. Given that there a number of newer Members following the election, training on this responsibility, and how breaches should be reported will be offered in due course.

1.22 An internal Corporate Governance Group has been set up recently, with the remit of critical friend and facilitator on governance and risk based questions. The group incorporates all chief officers and other key officers within the organisation. They will receive regular reports on information governance issues such as organisational data breaches, enabling more robust corporate scrutiny.

2. RISK MANAGEMENT ISSUES

2.1 A summary of the perceived risks follows:

Perceived risk	**Seriousness**	**Likelihood**	**Preventative action**
Non compliance, subsequent risk of financial penalty from the ICO.	High	Low	Continue to ensure compliance with ICO requirements within the information governance team. Continue to offer ongoing targeted training for teams with a high number of data breaches.
Resourcing and retention of skilled staff	High	Medium	Ongoing support to be offered to information governance team officers.
Reputational risk if a serious breach were to be reported	High	Medium	Continue to ensure awareness around the consequences of data breaches, and provide

			ongoing training to officers.
Likelihood of further data breaches	High	High	Regular reminders to be given to council officers on the importance of reporting breaches as soon as they happen, in order to meet ICO deadlines.

3. LEGAL/FINANCIAL AND OTHER CONTROLS/POLICY MATTERS

3.1 Legal Officer's Comments (AK)

The potential legal issues are covered in the main body of the report. It is vital that all officers exercise caution when handling data and any breaches are reported to the Information Governance team without delay so that appropriate action can be taken.

3.2 Finance Officer's Comments (TM)

There are no finance implications relating to this report.

3.3 Diversities and Equalities Implications (GE)

There are no equality and diversity issues directly arising from this report.

3.4 Climate Change Implications (OF)

There are no climate implications arising from this report.

4. CONTACT OFFICERS AND BACKGROUND DOCUMENTS

Councillors with any questions arising out of this report should contact the following officer prior to the meeting

Jemma West
Democratic Services Senior Specialist
01303 853369, Jemma.west@folkestone-hythe.gov.uk

Zoe Law
Case Management Lead (Corporate Services)
01303 853241, zoe.law@folkestone-hythe.gov.uk

The following background documents have been relied upon in the preparation of this report:

None.

Appendix 1 - Full breakdown of all reported breaches
Appendix 2 – Example of the new reporting features referenced at paragraph 1.18