UK GDPR – Notification of Data Breaches reported to the ICO

Jackie Tatam, Data Protection Officer

Report to:	**Audit and Accounts Committee**
Meeting date:	29 March 2021
Ward(s):	All
Key Decision:	**No**
Appendix 1:	**Confidential Appendix – details of breach**
Papers relied on:	**Data Breach Policy**

The Committee is invited to:

- Note the report.

Background, corporate objectives and priorities

The UK General Data Protection Regulation (UK GDPR) requires organisations to report serious personal data breaches to the ICO within 72 hours (of the organisation becoming aware of the breach) if it is likely there will be a risk to the rights and freedoms of individuals.

Where there is a high risk to the individual they must also be advised of the breach.

Failure to report a breach may result in action being taken against the council.

Glossary of terms

Term	Definition
UK GDPR	The UK General Data Protection Regulation
ICO	Information Commissioner's Office

Main considerations

1 Executive Summary

1.1 This report informs Members of the Committee that one serious breach has occurred since the last report which has been reported to the ICO. Details of the breach are contained within the confidential appendix to this report.

1.2 At the date of preparing this report, we have not received any further contact from the ICO regarding the breach.

2 Key issues for consideration

2.1 The Committee is invited to note the details of the breach and steps taken in response to the breach.

2.2 A further report will be provided to this Committee once the ICO has determined the breach.

Corporate implications

3 Legal

3.1 The council is required to comply with the GDPR and as such must ensure personal data is kept secure and handled appropriately.

3.2 All security incidents are investigated to determine whether a breach has occurred and, if so, the severity of that breach. Where necessary serious breaches are reported to the ICO.

3.3 The council is also required to comply with relevant data protection legislation in respect of the processing of personal data of its staff, Members, residents, customers and suppliers.

4 Financial

4.1 The ICO has the ability to impose monetary penalty notices of up to £17M in respect of serious breaches.

5 Risk management

5.1 A risk assessment has been completed in accordance with the council's risk management process and has identified the following significant (Red or Amber) residual risks that cannot be fully minimised by existing or planned controls or additional procedures. The main risks at this stage are as follows:

- Reputational damage following any adverse publicity resulting from the breach
- Monetary penalty notice being issued by the ICO

6 Equalities

6.1 There are no equalities implications arising from this report

7 Consultation and communication

7.1 This report has been completed in consultation with the Executive Director of Corporate Services and the Head of Law and Governance.

8 Climate change

8.1 There are no expected climate change implications arising from this report

9 HR

9.1 There are no HR implications arising from this report.

Conclusion

10 Summary and reason for the decision

10.1 The Committee is invited to note the content of this report.

Date: 29 March 2021

Decision taken by: Audit and Accounts Committee

Lead officer	Fiona Thomsen – Head of Law and Governance
Report author	Jackie Tatam – Data Protection Officer, ext 2369
Version	Final
Dated	4 March 2021
Status	Report Open Appendix Closed
Confidentiality	It is considered that information contained within the appendix to this report contains exempt information under the meaning of Schedule 12A of the Local Government Act 1972, as amended, and therefore cannot be made public.