56508

Please provide the following details for the period from 1 January 2020 to the most recent available date:

Number and type of cybersecurity incidents recorded.

In line with advice from the National Cyber Security Centre, we do not provide information relating to hardware, software and systems and therefore, unfortunately, it is not possible to provide you with the information you have requested.

While we can confirm that attempted cyberattacks occur on a daily basis, across all of the categories listed in your request, we will not be providing details of specific instances or numbers. Disclosing such information could highlight potential vulnerabilities and weaknesses and would therefore pose a risk to the security of our systems and data.

What we can confirm is that the Council operates a defence-in-depth approach to cybersecurity. This layered approach combines technical controls, continuous monitoring, and staff awareness to ensure that the vast majority of attempted attacks are identified and repelled before they can cause any harm.

As a result, while hacking attempts, phishing emails, malware/ransomware activity, and unauthorised access attempts are regularly observed, successful incidents are extremely rare and have limited the material compromise of the Council's systems during the period stated.

By providing such information about our IT services into the public domain we would potentially be putting our IT framework at risk. The public interest would not be served by the Council being subjected to the potential of Cyber attacks that could breach our security and damage our IT infrastructure.

Number of personal data breaches reported to the Information Commissioner's Office (ICO), including breaches relating to GDPR compliance.

	Availability	Confidentiality	Integrity	Total
2020	0	0	0	0
2021	0	3	0	3
2022	0	0	0	0
2023	0	3	0	3
2024	0	16	0	16
2025	0	6	0	7 (to date)*

*One breach reported to the ICO was that of the security incident of a third party who stated that the Council may be impacted by it. This was done as a precaution, and it may be the case the Council was not affected.

Details of breaches, including:
- Date of each breach
- Type of data compromised (e.g., names, addresses, medical records, financial details, employment data, etc.)
- Number of files or records leaked, compromised, or accessed without authorisation
- Whether the affected individuals were staff members, members of the public, or both

Number of individuals affected by each breach:
- Please break down by staff/public if applicable

By placing information in relation to the type of data compromised, number of files affected, and types of individuals affected into the public domain this would substantially prejudice the Councils ability to carry out its business as making such information public would have the effect of deterring members of the public and agency partners from passing such information to the Council.

Total financial compensation paid out to victims of data breaches, including staff and members of the public.

Total paid out for data breaches - £39,008
There has been a total of 8 claims with payments on them. The payments are inclusive of all fees, costs, and compensation, we do not have a breakdown which would separate these elements.

Brief summary of actions taken by your organisation to respond to each breach, including remedial or preventative measures.

The information is not held in the format requested. While the Council may hold this information in various disparate forms, it does not hold a singular record or summary of the actions taken. The Council's view is that to collate all this information would qualify as creating new information which is not required under the Act.