ARUN DISTRICT COUNCIL

REPORT TO AND DECISION OF AUDIT & GOVERNANCE COMMITTEE ON 19 NOVEMBER 2020

PART A : REPORT

SUBJECT: Data Protection Breach Overview

REPORT AUTHOR: Nicholas Bennett, Monitoring Officer & Data Protection Officer
DATE: 15 October 2020
EXTN: 37601
PORTFOLIO AREA: Chief Executives

EXECUTIVE SUMMARY:

The Council is responsible for protecting personal data that is collected, processed, stored and disposed of, in accordance with the Data Protection Act 2018.

Following a data protection breach that the Council became aware of in July 2020, the Information Commissioners Office (ICO) recommended that the Council minimised the risk of future data protection breaches, by raising awareness of the importance of Members and Officers being familiar with Council policies and completing mandatory training.

The Council is responsible for, and may receive a large financial penalty for, breaches of data protection.

All Members and Officers are individually accountable and may be prosecuted for data breaches.

RECOMMENDATIONS:

To recommend that Full Council note:

i) the summary of findings from the data protection breach;

ii) recognise, engage and fully endorse the importance of all Members and Officers completing mandatory training and adhering to policies, in order to minimise the risk of future data protection breaches;

iii) recognise that Council is responsible and accountable for breaches of data protection, and as such can face large fines, be liable to pay compensation, and suffer adverse reputational damage; and

iv) Council IT equipment should not be issued until the relevant security policies have been signed. In the case of re-elected Members who already have equipment, their accounts should be disabled until policies are signed.

1. BACKGROUND:

1.1 Following an incident after the Development Control Committee meeting had completed on 26 May 2020, the Chief Executive sent a several confidential communications to Members of that Committee and Group Leaders; All Members and

some Officers. He also wrote a non-confidential blog that is available to all Officers and Members.

1.2 The Littlehampton Gazette obtained copies of all of these communications, which revealed confidential personal data regarding disciplinary actions being taken against some Officers.

1.3 This data protection breach was reported to the ICO within 72 hours and investigated. Those Officers who had had information leaked about them were notified immediately. All Members and Officers who had been sent the emails were asked to confirm whether they had disclosed any or part of the information from those emails. All Members and Officers confirmed they had not made any disclosure.

1.4 ICT ran a security validation check on each of these email domains and confirmed that as they were all running government recommended email encryption protocols, they could not have been intercepted during transmission. However, once emails left the Council's email domain and had been received by the recipient, ICT could not track further. There was no evidence from that search that the data was provided to the Press directly from any Council system.

1.5 Those Members and Officers emails were also checked against to ascertain if they had forwarded any of those emails to an external private email address. This showed two Members had forwarded one of those emails to either (a) their own personal email address; or (b) a personal email address of another Member.

1.6 Those Members were contacted by email and asked to provide an explanation, and to refresh themselves on the policies they had breached by emailing private email addresses with personal data. They were also asked to complete the Information Governance & Cyber Security Training online by way of refresher.

1.7 It is acknowledged that any recipient of the emails could have printed these off and posted or passed these to the press.

1.8 Hampshire County Council also considered whether any further steps could be taken in the investigation and recommended that when appropriate, emails are marked 'confidential'.

1.9 The Council's policies were considered robust, provided they are followed, to minimise the risk of data protection breaches.

1.10 It is noted that all Officers must read the Information Security Policy and Internet & Email Acceptable Usage Agreement upon commencement of their employment with the Council; it is their individual responsibility to ensure compliance with this. Similarly, following the election in May 2019, all appointed Members were asked to sign up to the Council's Information Security Policy and Internet & Email Acceptable Usage Agreement when provided with ICT equipment. However, this has proved difficult to obtain Member sign up.

1.11 The ICO considered the breach and decided no further action would be taken on this occasion, concluding there was insufficient evidence to substantiate a criminal offence.

1.12 The ICO provided reasons for their decision as follows:

- This looks to have been an isolated incident affecting a limited number of data subjects and does not appear to indicate a broader data protection compliance issue within your organisation;
- At the present moment your organisation are unaware of the source of the leak and your investigations into this issue are ongoing;
- Your organisation are intending to contact potential sources of the breach as part of your organisation's investigation into this incident;
- You have indicated action you will take in order to prevent a recurrence of this incident, including requesting that members of staff complete data protection training.

1.13 The ICO recommended:

1) Ensuring that everyone completes mandatory data protection training. As an organisation, it is our responsibility to ensure that any personal data handled within our organisation is secure and that Members/ Officers are aware of what they can and cannot do with the data they come into contact with;
2) Reviewing the preventative measures the Council had in place prior to this incident and establishing why these measures proved ineffective in this instance;
3) Continuing to monitor this incident in order to ensure awareness of any potential risks to the rights and freedoms of the data subjects as a result of this incident, and any actual detriment caused.

1.14 Actions taken:

- A check was made that all Officers and Members had completed the mandatory Dojo training on Information Governance & Cyber Security. A number of Members and Officers have yet to complete the training.
- On 10 August 2020, Alan Peach, Group Head of Corporate Support, emailed Councillors who had not yet signed up to the Council's Information Security Policy and Internet & Email Acceptable Usage Agreement, asking them to do so by the end of August. There were some issues reported accessing links which ICT resolved. Reminders were issued in September; by the end of September 2020 all Members had signed up. It has taken a lot of resources to follow up and ensure all Members had signed up, since May 2019 – September 2020.
- Members may wish to consider how promptly sign up should incur to these policies in future, and what should happen if any Member does not sign up, given the significant consequences on the Council of any data protection breach. More stringent monitoring of sign up to policies is required in future.

1.15 As you are aware, the Council is required to have appropriate technical and organisational measures in place to ensure the security of personal data. The Council is responsible for protecting personal data that is collected, processed, stored and disposed of, in accordance with the Data Protection Act 2018. The Council often deals with large amounts of highly sensitive data regarding their constituents, so the scope for damage can be considerable. The Council is responsible for breaches of data protection, which is enforced by the ICO. The ICO can fine an organisation up to 20 million Euros, or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher. The Council can also suffer huge reputational damage from

breaches of data protection and lose the trust and confidence of its residents. It may have to pay compensation.

1.16 There is also individual accountability as you may be held personally accountable for a breach. It is therefore of paramount importance that all Members and Officers ensure they are familiar with, and comply with, the relevant policies.

1.17 To minimise the risk of data protection and freedom of information breaches, and the potential consequences to the Council and Officers and Members individually, the Council has in place polices and mandatory training for all. Breaches of data protection should be reported immediately to the Information Management Team, using the online e-form. Nicholas Bennett is acting as Arun's interim Data Protection Officer. For advice and assistance, contact: data.protection@arun.gov.uk

2. PROPOSAL(S):

To recommend that Full Council note:

i) the summary of findings from the data protection breach;

ii) recognise, engage and fully endorse the importance of all Members and Officers completing mandatory training and adhering to policies, in order to minimise the risk of future data protection breaches and

iii) recognise the Council is responsible for breaches of data protection and can face large fines and suffer reputational damage.

3. OPTIONS:

To recommend Full Council note the recommendations listed, or not.

4. CONSULTATION:

Has consultation been undertaken with:	**YES**	**NO**
Relevant Town/Parish Council		**No**
Relevant District Ward Councillors		**No**
Other groups/persons (please specify)		**No**

5. ARE THERE ANY IMPLICATIONS IN RELATION TO THE FOLLOWING COUNCIL POLICIES: (Explain in more detail at 6 below)	**YES**	**NO**
Financial	Yes	
Legal	Yes	
Human Rights/Equality Impact Assessment		No
Community Safety including Section 17 of Crime & Disorder Act		No
Sustainability		No
Asset Management/Property/Land		No
Technology		No

Other (please explain)	Yes - Data Protection Officer	

6. IMPLICATIONS:

Finance

Size of fines as noted in the report.

Legal

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018 closely followed by the Data Protection Act 2018. This legislation brought in new requirements for the Council to consider about how it put the privacy of the personal information it holds higher on its agenda; gave individuals additional rights to how their personal information is managed; and increased the level of fine that the Council could face if it breached the law.

Data Protection Officer

Members are reminded that under the Data Protection Acts and the GDPR they are subject to individual responsibilities to apply proper care to information. They are subject to statutory duties as Data Processors in their own right (when acting as a Councillor outside of a Borough Council process) and further that they are subject to enhanced duties as to confidentiality. If a councillor has accessed information under the common law 'need to know' on which much information is shared with them by officers, then in most cases the information may still be confidential and the councillor bound by confidentiality. In that case they should not publish or otherwise disclose the information to a third party. Each of these duties requires proper policies to support and clarify these general legal responsibilities.

7. REASON FOR THE DECISION:

To minimise the risk of data protection breaches in order to safeguard the Council's reputation and finances.

8. BACKGROUND PAPERS:

Information Commissioner's Office website: https://ico.org.uk/