Report to: Cabinet

Date of Meeting 20 January 2021

Document classification: Part A Public Document

Exemption applied: None

Review date for release N/A

Councillor password data breach

Report summary:

This report is to update members and the public following the discovery and subsequent reporting of Councillor passwords being visible in November 2020.

Recommendation:

That Cabinet note the content of the report and confirm whether they are happy with the position that has been reached or whether further independent reassurance is required.

Reason for recommendation:

It is considered that the Strata Investigation Report and commentary in this report should reassure members around the concerns that have been raised. If it doesn't then members have the option to seek further reassurance.

Officer**:** Henry Gordon Lennox, Data Protection Officer

Portfolio(s) (check which apply)**:**
☐ Climate Action
☐ Coast, Country and Environment
☒ Corporate Services and COVID-19 Response and Recovery
☐ Democracy and Transparency
☐ Economy and Assets
☐ Finance
☐ Policy Co-ordination and Regional Engagement
☐ Strategic Planning
☐ Sustainable Homes and Communities

Financial implications:

There are no direct financial implications from the recommendations in the report.

Legal implications:

The legal implications are appropriately detailed in the report.

Equalities impact Low Impact

Climate change Low Impact

Risk: Low Risk;

Links to background information None

Link to Council Plan:

Priorities (check which apply)

☐ Outstanding Place and Environment
☐ Outstanding Homes and Communities
☐ Outstanding Economic Growth, Productivity, and Prosperity
☒ Outstanding Council and Council Services

Report in full

1. On 10th November 2020, it was discovered that password information relating to some Members was capable of being seen by other Members. The password information pertained to Office 365 users and also another piece of software the Council uses. The matter was immediately reported to Strata who commenced an investigation.

2. During the early stages it was not evident the extent of the issue but quite obviously it represented a clear risk in terms of information security and data protection issues. Early mitigation steps were taken to resolve the issue including ensuring the erroneous display of the passwords being corrected so that they could no longer be seen and all the potential affected users being contacted to change their passwords.

3. On the 11th November Strata reported the matter to the Information Commissioner's Office (ICO) as a reportable data breach. The Leader also issued a communication to all members informing them of the incident and steps being taken. That email informed members of an investigation being taken by Strata and that a report to Cabinet would follow.

4. On 26th November the ICO closed the matter and the content of the email from them is contained at Appendix 1.

5. Strata have completed their investigation with a large amount of help and input from Members and of course their officers, which is appreciated and acknowledged from perspective of DPO for East Devon.

6. While the investigation was underway, the breach came to the attention of the press and it was subsequently reported (on the DevonLive and BBC websites) by them and in so doing they inaccurately stated that Member passwords had been made publicly available and also revealing other sensitive information. Steps were taken by the East Devon communications team to correct the inaccuracies.

7. This report follows on from the email from the Leader and the inaccuracies reported in the press. Copied below is the Executive Summary from the Strata Investigation Report written by the Strata IT Director to provide reassurance to Members and the public regarding this incident.

Executive Summary – Laurence Whitlock, Strata IT Director

This Executive Summary is based on the investigation and findings of the Strata Head of Security and Compliance into the disclosure of EDDC Councillor password information. Such incidents are treated seriously by Strata. It is clear that once notified of the disclosure, Strata reacted very quickly and professionally in mitigating the risk and identifying the root cause.

The key critical point is that it can be confirmed that external visibility of the password information by individuals residing outside of the Strata provisioned Office365 environment would not have been possible, primarily because of the secure way in which

the Strata Office365 environment has been designed, built and deployed. Hence, Strata can confirm categorically that there was no public visibility to the password information. In addition, the likelihood of Councillor passwords and emails being compromised by other Councillors appears very low and any misuse of the password information would have been in contravention of the Computer Misuse Act 1990.

The investigation into the password disclosure was carried out using logs for a three-month period (Office 365 platform only holds comprehensive log information for a three-month period). There is no evidence to suggest that there has been any unauthorised or malicious use of passwords during the log period of 11th August 2020 until 13th November 2020. In all likelihood, had there been any unauthorised activity prior to the log period, this would have continued during the log period itself. Although it is conceivable that password visibility to other Councillors could have potentially been from end of Sept 2019 until early October 2019 (when the O365 migration took place to the start of the log period in August 2020), based on Strata's investigation coupled with Strata's determination of the likely timeframe when the passwords actually became visible, it is Strata's professional judgement that in reality the likelihood of the passwords having been compromised by other Councillors at any time is very low.

The investigation identified the possibility of 36 Councillors who may have had visibility to the password information due to their use of the Strata Office365 environment. However, investigation revealed that it was only Android users (whether using the Android app or accessing Outlook.com on the Android web browser on the Android device) who could see the information and hence this further limited accessibility. Analysing the log information indicated that there were only 7 active Android users during the three month investigation period.

Strata reported the incident to the Information Commissioners Office (ICO), who have reviewed the case and due to the speed of the Strata response and the controls in place, the ICO have concluded no further action is necessary and the case has been closed.

In conclusion, the root cause of the incident was rapidly identified by Strata and corrective measures put in to place immediately and there was no wider risk of threat to the Council's IT systems. There are a number of key lessons learned and recommendations that have been identified as result of this incident:

1) Councillors need to be provided with the ability to manage their own passwords, irrespective of how complex the delivery of such functionality is. Whilst this may make the support of Councillor devices and applications more difficult, a solution to this issue needs to be identified, procured and implemented;
2) Strata security practices need to be reviewed regularly to ensure that there are no weaknesses in access controls;
3) The security of data and in particular passwords is all staff's responsibility and any evidence of poor practice should be reported immediately.

Strata apologise that this issue occurred and we would like to reassure members that we will continue to strive to work both professionally and diligently in our delivery of IT services to East Devon District Council.

8. AS DPO for East Devon, having regard to the ICO position, I am reassured by the response and actions of Strata in dealing with this incident and that the future mitigation actions and recommendations in their report will ensure that there is a very low risk of this incident or similar occurring again. As DPO I will be proactively ensuring that the identified steps are delivered.

9. During discussions in relation to the specific incident addressed above, concerns were raised regarding the Member induction programme in May 2019 and the view that there was a spreadsheet containing Member's passwords and also a prioritisation system.

Concerns were expressed about these passwords being capable of being seen by other Members. Having investigated within Democratic Services and asked Strata to investigate from their perspective I can confirm the following;

(1) The Council had agreed to roll out iPads to the new Council membership following the 2019 election. Despite a number of members being re-elected, all 60 councillors were to have the equipment rolled out and it wasn't known who they would be until after the election.

(2) An induction session was organised the purpose of the meetings was to ensure that all the councillors elected in May 2019 were provided with and able to access computer equipment to facilitate the use of the Council IT systems. Predominantly the sessions were about setting up the iPads, iPad basic training, ensuring access to Council emails and also being able to use the Modern.Gov app (this is essentially committee related) and logging into the extranet to enter register of interests.

(3) The Councillor induction / roll out was carried out over two days and four sessions in the early part of the week after the election results which were returned on the Friday. Strata therefore had to progress equipment preparation for the 60 Members at East Devon and also members at Exeter and Teignbridge in a very tight timeframe.

(4) As Modern.Gov is 'owned' by Democratic Services and in order to assist Strata in preparing the roll out a spreadsheet was created in Democratic Services which contained information relating to who the Member was, the preferred email address and contact details amongst other information. It also contained a priority lettering (A-D) against each Councillor which simply identified which of the four welcome sessions the Councillor was attending to enable Strata to manage their workflows and prepare the equipment in time. It also contained a password to Issue Manager (essentially the Modern.Gov app on the iPad). The spreadsheet was passed to Strata to enable them to carry out the preparation work. The spreadsheet was seen / used by two Democratic Services staff members and four Strata officers from the implementation team.

(5) In attendance at the induction sessions were Democratic Services and Strata officers. The spreadsheet was used during the sessions to help members with their passwords for Modern.Gov. It is accepted that there was the possibility for members to have seen the passwords if they were looking at the sheet being used. It has also been reported (by a Councillor) that when attending Blackdown House for IT support, they were left in front of a screen in the Strata Service desk area where the list was displayed.

(6) No other password was visible to Members outside of Issue Manager at that time.

(7) Subsequently there were issues with the Council equipment and its functionality and so in Sept / Oct some Members were migrated to Office 365. In that transfer a password very similar to the Issue Manager passenger was used – on the basis that having lots of different passwords can cause difficulties not least in remembering them.

10. As DPO it is accepted that because some Members were able to see the Issue Manager password that this represents a technical data protection breach. It is clearly poor practice not to protect sensitive information from those not entitled to see it (such as covering up the sheet or locking a computer). However, the information that this password would enable anyone to see (essentially Modern.Gov) is information Members can all already access. If a Member did take note of another Member's password in May 2019 there is nothing else that they could have used it to access. Given the likely small number affected and foregoing, the risk that this presented was extremely low.

11. Turning to the use of a similar (sequentially numbered password) in the transfer to Office 365, this is not a data breach as no personal data was revealed to anyone. However, it is accepted by Strata that this was also not good practice. Moreover, for anything untoward to happen it would require a Member to have remembered another Member's password, be someone who was transferred to Office 365, appreciated the approach used and then sought to use that information to access another Member's account.

12. The commentary in the Strata report in relation to the recent incident is as equally applicable to the concerns surrounding the transfer to Office 365. The biggest deterrent is of course the criminality of accessing someone's account without permission but it is also worth noting that Councillors are trusted individuals and this is in itself part of the rationale of concluding that unauthorised access is highly unlikely to have occurred.

13. Returning to the spreadsheet, from DPO perspective there is no issue with the creation of this or the keeping of passwords within Democratic Services for accessing Modern.Gov. In carrying out the investigation I did try to access the spreadsheet in the Committee folders in the Council computer drives but it is locked and access is restricted to the two Administrators for Modern.Gov. The issue of others being able to see passwords in a list and the use of similar passwords is clearly poor practice and steps, such as appropriate training and reminders to staff, will be undertaken to seek to avoid a repeat event.

14. Hopefully the above reassures Members (and the public) that the password incident and issue surrounding the spreadsheet has been appropriately investigated, concerns addressed and steps identified to prevent reoccurrence. If Members remain concerned then it is within your gift to request additional or independent audit of the matters.

Appendix 1 – Email from the ICO dated 26th November 2020

Reference Number [redacted]

[redacted]

I am writing further to your personal data breach report of 11 November 2020 regarding password and contact information being visible through Office365 affecting up to 150 people.

Thank you for the information you have provided.

Data security requirements

You are required to have appropriate technical and organisational measures in place to ensure the security of personal data.

Our Decision

We have considered the information you have provided and we have decided that no further action by the ICO is necessary on this occasion. This decision is based on the information we have recorded about the breach.

The reasons for our decision are as follows:

- It appears that the information was exposed to a limited number of people, and technical logs have shown that there has been no incorrect access to the data. This could reduce the risk to the data subjects.
- You have determined that the personal data breach is not likely to result in a high risk to the data subjects.
- It appears you have the appropriate technical security measures in place to protect the personal data you process.
- After discovering the incident steps have been taken to remove the information and to sycronise the system to contain the breach. Additional steps have been taken to change passwords to prevent any unauthorised access.
- You have advised that the root cause of the incident was process based and you have changed your process for recording information to prevent another incident of this nature.
- It is noted that all sensitive data has been removed, which could reduce the risk of this information being disclosed.

However, we recommend that you investigate the causes of this incident, to ensure that you understand how and why it occurred, and what steps you need to take to prevent it from happening again.

In particular, we recommend that you consider:

- Ensuring that any changes to your processes are communicated consistently with all relevant staff and training is provided. Your processes should be well documented and this guidance should be easily accessible.

- Continue to review your processes and make any improvements or changes where necessary. There should be robust checking measures in place when setting up equipment to ensure all the relevant security measures are applied, and they are setup correctly.
- Reminders should be issued to all relevant staff on a regular basis of the importance of data protection, their responsibilities, and the correct process to follow. This could be done through email updates, bulletins on an internal site, or during staff meetings.
- You should consider conducting regular audits or spot checks of the system, which could help identify any vulnerabilities to prevent any further disclosures.

The ICO recognises the unprecedented challenges many organisations are facing during the Coronavirus (COVID-19) pandemic, and are reflecting this in our processes. We understand that in some cases, resources might be diverted away from usual compliance or information governance work. We fully understand this may lead to a delay in your investigation being completed and implementation of the recommendations listed. Therefore, we ask you to complete them as soon as you are able to, as this will help to protect the personal data you hold from similar occurrences in future.

Please also note that as a result of a breach an organisation may experience a higher volume of complaints and information rights requests. You should not refer them to the ICO as a matter of course, and it is important that you deal with these, alongside the other work that has been generated as a result of the breach. However, we do recognise some organisations may experience delays in dealing with these requests at this current time, we have advised data subjects they may see delays whilst organisations prioritise tasks, you can read more about this on our Coronavirus information hub.

Thank you for reporting the incident. Further information and guidance relating to data security is available on our website.

Please note that we may make additional enquiries if we become aware of new information which affects the circumstances of this case.

We now consider the matter to be closed.