FULL COUNCIL

22 NOVEMBER 2022

REPORT OF DEPUTY LEADER OF THE COUNCIL & PORTFOLIO HOLDER FOR CORPORATE FINANCE AND GOVERNANCE

A.9 INFORMATION GOVERNANCE

(Report prepared by Richard Barrett and John Higgins)

PART 1 – KEY INFORMATION

PURPOSE OF THE REPORT

To present to Full Council an update on proposals for IT changes. The ongoing work is aimed at reaching an outcome whereby members can undertake their role effectively, whilst ensuring that information held by the Council, is safe, secure and compliant with relevant legislation. This work will also include looking at various different IT solutions and the associated costs.

EXECUTIVE SUMMARY

Like all modern twenty-first century organisations, the Council is reliant upon information, data and digital services to deliver all our services. The Council securely stores and holds guardianship over some 60 terabytes of residents', customers', visitors', members' and officers' personal and special category data. To put this into context, 60 terabytes of data represents the equivalent of 390 million document pages or 15 million digital photos.

Members are reliant upon access to their emails to undertake their role as a Councillor. Members also have a responsibility to ensure that the sometimes sensitive personal or organisational information they are sent is kept safely and respects its confidentiality.

Throughout 2018-2021 the Council's IT Service implemented and achieved compliance with increasing NCSC technical security standards. The UK adopted its UK Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) legislation on 25 May 2018.

The key Principles of UK Data Protection legislation require that the data is stored: **lawfully, fairly** and **transparently**, **adequate** and **relevant** and **limited** to what is necessary, **accurate** and where necessary kept up to date, **kept for no longer than is necessary** in a form which permits identification of data subjects, **ensuring 'integrity and confidentiality'** protecting against unauthorised or unlawful processing and against accidental loss/ destruction/ damage **through using appropriate security**.

Processing of personal data *- means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

The Department of Levelling Up Housing and Communities (DLUHC) commenced local authority security resilience audits in 2021. In December 2021 the DLUHC 'Health Check' scan identified the Council's auto-forwarding of emails practice and recommended that the

practice be phased out a soon as possible. These DLUHC local government cyber-security audits are being rolled-out to all authorities during 2023.

The DLUHC audit was considered and agreed by the Audit Committee and the March 2022 Corporate Risk Register reported the need to cease the practice of auto-forwarding of Councillors' emails. The minutes of the Audit Committee were reported to Full Council in July 2022.

The UK Data Protection legislation (6th Principle) requires that information and data are processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss/ destruction/ damage through using appropriate technical or organizational measures (integrity and confidentiality). In all matters of council business, the Council is the Data Controller and has legislative responsibility to ensure, and to evidence, that information is being managed and protected in accordance with the principles of the legislation.

The risk of cyber-attack is not new, but it is escalating in terms of frequency, severity and complexity. To counter these sophisticated attacks the Council's protected domain uses a range of best of breed, commercial-grade security services from multiple vendors.

The original proposal of ceasing auto-forwarding of emails was met with concern from some members as they felt it might curtail their ability to access information and fulfil their role. Therefore, the Portfolio Holder has instructed Officers to explore different solutions (including some new processes of creating an app for members to be able to access their emails securely on their own devices), whilst being mindful of ensuring the security of such information and protection against cyber-attacks.

Scrutiny has included Cyber-security in the work programme. In consultation with the Chair of Scrutiny, (Councillor Mark Stephenson), it is proposed that the remit be extended to include the issue of members' access to their information and the alternative solutions available, mindful of the recommendations of Audit Committee and the issues of confidentiality, Data Protection and cyber security. With all members having the opportunity to have an input and recommendations being brought back to a future Council meeting.

The original proposal to cease the auto-forwarding of emails emerged from an information governance / GDPR review undertaken by Internal Audit. The associated review, which supported this approach, was undertaken in line with the Council's existing risk management processes and included input from the Council's Data Protection Officer, S151 Officer, Internal Audit Manager and Senior Information Risk owner (SIRO). The risk management process highlighted above included the Council's Audit Committee, who after considering the matter at its January 2020 meeting, resolved that:

> ***The Committee supports the implementation, as soon as possible, of the proposal set out within the report for providing the necessary IT equipment and training to Members to ensure that only Council equipment is used when conducting Council business in order to reduce the financial and reputational risk associated with processing personal data.***

Although in a wider context, the matter also formed part of a report that was considered by the Resources and Services Overview and Scrutiny Committee at its meeting in January 2021.

Whilst this additional work is being explored, Members acknowledge that the ongoing risk of the Council, acting as Data Controller, potentially in breach of the Data Protection Act 2018 remains, whilst the auto-forwarding of Councillor emails practice continues. Individual Councillors may however voluntarily request that auto-forwarding is ceased for their email account, which is maintaining the status quo and has been adopted by 20 councillors.

The Council has all-out elections in May 2023, so it is proposed that all changes be implemented for the new Council in 2023.

It is also proposed that a workshop be scheduled for all members to highlight the requirements of Data Protection and the prevalent issues cyber breaches and security requirements. This will assist in mitigating the risks of breaches.

In terms of the proposed review by the Resources and Services Overview and Scrutiny Committee, it is worth highlighting the Councils' existing adopted Risk Management Framework seeks to address a number of key elements such as the identification of risks, the analysis of those risks and whether they can be 'tolerated' or need to be 'treated etc., with the latter including reviewing potential options. With the above in mind, it would seem logical / pragmatic to structure the proposed review around these existing risk management principles, which would have formed part of the original work undertaken by Officers and the Audit Committee. This approach would also complement a wider review of various cyber related issues as part of the Cyber Assessment Framework recently published by the National Cyber Security Centre (NCSC) that was considered at the first meeting of the relevant Resources and Services Overview and Scrutiny Committee Task and Finish Group on 27 October 2022.

Subject to the recommendations below, Members are invited to submit any comments or thoughts on the subject of cyber security and email forwarding for the Resources and Services Overview and Scrutiny Committee Task and Finish Working Group to take into consideration. This can be done via email to Democratic Services at democraticservices@tendringdc.gov.uk

RECOMMENDATION(S)

It is recommended that:

1. **Full Council acknowledges that the ongoing risk of the Council, acting as Data Controller, potentially in breach of the Data Protection Act 2018 remains, whilst the auto-forwarding of Councillor emails practice continues;**
2. **the Resources and Services Overview & Scrutiny Committee extend its work programme of cyber security to include reviewing the different proposals of Members' access to emails, in line with the Council's Risk Management Framework, and make recommendations to Cabinet and Council along with relevant costings;**
3. **such proposals to be mindful of the recommendations of the Audit Committee, Data Protection Act requirements and cyber security;**
4. **a workshop be scheduled for all Members to ensure awareness of the requirements of the Data Protection Act 2018 and cyber security; and**
5. **the implementation be planned for no later than 1st April 2023 in readiness for the commencement of the new Council, following the elections in 2023 and the new Councillors be given the training as detailed in 4 above.**

BACKGROUND & PREVIOUS DECISIONS

As communicated to Members recently, one of two key actions relating to Members use of IT, which has been deferred, is as follows:

Stopping the practice of auto-forwarding council emails and official data to personal email accounts outside of the Council's protected domain.

The other key action recently implemented was as follows:

Locking down access to all council applications and non-public facing systems to council managed devices only within our council protected domain. (which came into effect on 29 July 2022)

Both actions should be viewed as complimentary actions, as auto forwarding of emails would present an immediate conflict, as emails sent to an official Tendring email account would instantly leave the Council's 'protected' domain. This point underpins the recommendation raised via the audit process below which concentrates on the underlying issue of only using a Council managed device when undertaking Council business.

A summary of the background to the associated governance and reporting actions within the Council to date are as follows:

20 January 2020 - Following an information governance / GDPR review, a report of the Head of Internal Audit was considered by the Audit Committee. Within that report, the following issue was set out.

An issue of non-compliance with the Data Protection Act 2018 was identified for consideration along with proposed actions by the Audit Committee.

There have been occasions in the past where personal and special category TDC data has been forwarded to personal emails by both Officers and Members. It is however recognised that this is for ease of use rather than anything malicious. However Data Protection Act 2018 legislation, particularly Article 5, Paragraph 1(f), requires personal data to be "processed in a manner that ensures appropriate security of the personal data". We are unable to demonstrate compliance in this regard as personal devices and their cyber-security remain outside of the sphere of Council knowledge, control and management. It is therefore recommended that Officers be reminded of the need to ensure that TDC data be retained within TDC encrypted, secure 'official' emails and not forwarded to personal emails. In respect of Members, the recommended control is that only Council issued equipment and email addresses should be used to prevent the need of forwarding data to personal emails and increasing the risk of non-compliance and the wider financial and reputational consequences if personal data is not secure.

Following consideration of the above, the Audit Committee resolved:

The Committee supports the implementation, as soon as possible, of the proposal set out within the report for providing the necessary IT equipment and training to Members to ensure that only Council equipment is used when conducting Council business in order to reduce the financial and reputational risk associated with processing personal data.

The minutes from the above meeting were included within the Full Council agenda on **15**

September 2020.

29 May 2020 – As part of a review of the Council's Constitution, Cabinet considered an associated report where the following resolution was agreed:

That Cabinet endorses that all Councillors conduct all Council business through their Tendring District Council online accounts using the corporate IT kit supplied to them for the smooth facilitating and running of remote meetings.

15 September 2020 – The above was included within the various documents considered by Full Council as part of formally agreeing a number of changes to the Council's Constitution.

3 December 2020 - Members may also recall various discussions relating to using Council managed devices, when previous devices such as Microsoft Surface GO's were replaced with laptops, a key action in supporting the move to restricting system access to only Council managed devices. This was a matter that was considered by the Resources and Services Overview and Scrutiny Committee at its meeting its meeting in December 2020.

The record of the discussion as set out in an extract from the minutes of the meeting is as follows:

The emerging digital picture was therefore, perceived as an opportunity to assist councillors in their community leadership role. Through providing each councillor with a standard, managed device backed up by IT training and supported via the Council's IT service desk intended benefits and improvements were, and remain, as follows:

- *To assist Councillors to improve their efficiency and access to stored digital information.*
- *Strengthen cybersecurity (and cybersecurity awareness) and further reduce any possibility of a data breach and Information Commissioner's Office (ICO) data loss.*
- *Enhance Councillors' digital engagement.*
- *Enhance mobile working and flexible working capabilities and thereby work/ life balance*
- *Further reduce reliance (and the costs) of printed information.*
- *Councillor IT equipment standardisation would in turn enable officers council-wide to standardise the range services that they provide which would achieve efficiency savings for both Councillors and Officers.*

Members heard how the strategy had been to purchase high quality Microsoft Surface Go tablets during 2019 and at the beginning of 2020 for Councillors to undertake their council-related duties. With some Councillors struggling with the tablet screen size Officers had additionally offered Councillors: connection hubs, full size keyboards, 24" screens, cabled mouse. This gave Councillors a blend of home-based digital access with the ability to go mobile with their tablets when required.

As a result of COVID-19 and an emerging understanding as to its longevity, officers had become conversant with new face-to-face restrictive working arrangements and the use of virtual Microsoft Skype meetings had become a key 'new working norm'. Likewise, virtual meeting MS Skype capabilities had needed to be extended to Councillors to enable them to perform their duties, which was not an intended original use of the previously purchased tablets.

The Committee was informed that the Council now had a pressing financial, technological and

support need to migrate fully from Microsoft Skype to Microsoft Teams. Teams offered a range of additional meeting business functionality benefits over Skype but it was far more demanding in terms of computing processing power. As such, it was close to the limit and was very likely to become beyond the processing capabilities of councillor tablets as Microsoft invested in further enhancing Teams functionality.

With a view to giving Councillors the very best experience possible during multi-party video conference calls, the decision had now been taken to allocate funding to quickly replace Councillors' tablets with the same Lenovo laptops that officers used. Those laptops were tried and tested, high specification devices that had enabled officers to perform the full range of council business demands.

The Committee was also informed in addition, and based upon approaches from several senior Councillors, that providing Members with a council tablet had unintentionally been seen as an 'imposition' by some Councillors, despite Officers' best intentions. Likewise, Officers had now acknowledged Councillors' desire to be increasingly involved in their use of digital technology and how they worked and engaged with council business.

With engagement firmly in mind but reflecting the need to standardise equipment across Officers and Councillors as far as was possible, Councillors would now be asked on an individual basis whether they would benefit more from having a smaller, lighter more portable 13" council laptop, or a larger 15" laptop with a bigger screen and near full-size keyboard. Council provided ancillary devices – keyboards, screens, mice, hubs – would continue to be offered to Councillors and those who already had them would be able to connect and continue to use them with their replacement laptops.

Following the consideration of the above, the Committee resolved:

That the Cabinet be informed that this Committee endorses the principle that Councillors be consulted on the IT kit that is to be provided to them to fulfil their roles as Members.

29 January 2021 - The consultation process was undertaken as highlighted above along with Cabinet considering the above comments from the Resources and Overview and Scrutiny Committee at their meeting in January 2021, where the following comments from the Portfolio Holder for Corporate Finance and Governance were included and endorsed:

I thank the Committee for their comments, and I am delighted to state that all Members of the Council have now been furnished with a brand new device of their individual choice. The roll out of these during the current lockdown has been carried out impeccably by our IT guys, who going by the comments I have personally received and fed back form colleagues, have done this in safest possible manner, and for which I am very grateful."

The Council maintains a Corporate Risk Register that is reviewed on a 6 monthly cycle by the Audit Committee. The two relevant risks included within the register are as follows:

- Ineffective communication / management of information
- Ineffective Cyber Security Physical and Application (software) Based Protection Management

Updates against the Committee's earlier recommendation from their January 2020 meeting have been included within these reports with the following extracts worth highlighting:

27 May 2021 - *Whilst our information governance continues to strengthen, the Information Commissioner's Office (ICO) continues to 'raise the bar' on compliance matters. We are currently reviewing how Councillors access, utilise and manage personal and sensitive information and we must work to introduce changes to Councillor working practices to strengthen this aspect of Council information governance during 2021 or risk being found potentially in breach of General Data Protection Regulation legislation by the ICO. The key issue here is that having provided every councillor with a managed council device we must cease the councillor practice of forwarding council emails to personal email accounts where we have no control over cyber security protective measures. Ongoing vigilance with regard to Information Governance resources and training and budget to minimise the risk of an information breach or failure to comply with legislation as this work area volume increases significantly.*

31 March 2022 – *The above matter was highlighted during a cybersecurity audit by the Department for Levelling Up Housing and Communities (DLUHC) as a significant cybersecurity risk that must be ceased. We will therefore work to achieve this during early 2022 in a supportive manner with additional training provided if required.*

12 July 2022 - The minutes of the above Committees were reported to subsequent Council meetings, with the latest minutes being presented to their meeting in July 2022.

In support of the above, a note was recently sent to all Members as part of the Chief Executive's regular member briefings to provide advance notice of the proposals to cease the automatic forwarding of emails and access to the Council's network from a non-TDC managed device.

The culmination of the above was the email recently sent to Members highlighting the proposed implementation of the two key actions set out at the beginning of this section of the report. The deferral was requested by Members to allow a debate at Full Council to take place.