COUNCIL

2 MARCH 2023

REFERENCE FROM THE CABINET

A.4 CYBER SECURITY FOR THE COUNCIL

(Report prepared by Ian Ford and Keith Simmons)

PART 1 – KEY INFORMATION

PURPOSE OF THE REPORT

Further to the decisions of Council on 22 November 2022 (Minute 55 refers), to receive recommendations arising from the Overview and Scrutiny enquiry into cyber security together with the outcome of the consideration of those recommendations by Cabinet on 17 February 2023 (Minute 122 refers).

EXECUTIVE SUMMARY

In accordance with the above decision of Council on 22 November 2022 (referred to above), the Resources and Services Overview and Scrutiny Committee extended its work programme enquiry cyber security to include reviewing the different proposals of Members' access to emails, in line with the Council's Risk Management Framework. The enquiry was undertaken by a Task and Finish Group comprised of Councillors Clifton (Chairman), Amos, Coley, Griffiths and Wiggins. The Task and Finish Group met four times and submitted its report to the Resources and Services Overview and Scrutiny Committee at a meeting of that Committee on 1 February 2023.

The Resources and Services Overview and Scrutiny Committee, pursuant to the decision of Council on 22 November 2022, submitted its recommendations arising from the cyber security enquiry to Cabinet on 17 February 2023 and also to this meeting of Council. That Committee recommended –

"That Cabinet –

a) requests, that as soon as is possible, the Human Resources and Council Tax Committee with appropriate officers looks at the salaries being offered for the advertised and unfilled senior IT posts, including cyber security senior technical positions;

b) endorses that by 31 March 2023 a Portfolio Holder Cyber Security Working Group be established to periodically review the Council's cyber security performance against the Cyber Assessment Framework (CAF) and/or emerging mandatory security improvements and requirements;

c) requests that by 31 July 2023 the Council's Information Retention Policy be reviewed/ revised with due regard to UK Data Protection Act 2018 data 'minimisation' 'accuracy' and 'storage limitation' and applied throughout the organisation;

d) requests that by 31 May 2023 individual (non-generic) account access technologies be costed for accessing TDC terminals in locations such as leisure centres where numerous users sharing a terminal due to a retail environment operational need;

e) requests that, commencing no later than May 2023 following the election of the new Council, Cyber Security and Information Governance training for all Members after every election and for staff in their inductions be introduced with periodic refresher training for both which will be made mandatory;

f) requests the Council's Monitoring Officer to review existing Member guidance and explore Member training opportunities as to what constitutes party political activities in the context of using a TDC email account;

g) endorses that as soon as possible the new Cyber Incident Response Plan (CIRP) be adopted.

That Cabinet recommends to Full Council that –

h) post-May 2023 local elections under the newly elected Council that Members' practice of auto-forwarding of emails be ceased;

i) subject to the associated funding of £8,000 being identified, that the preferred Option 2 i.e. the provision of a standard council-managed mobile Smartphone in addition to a council-managed laptop be provided to those Members that want one to access emails and to be contactable when mobile; or

j) as an alternative to i above, that should it not prove possible to fund the Smartphone costs centrally, then each Member requesting a standard council-managed mobile Smartphone be asked to fund the cost from their Allowances (circa two hundred pounds per annum)."

Cabinet had before it at its meeting held on 17 February 2023 the following comments submitted by the Portfolio Holder for Corporate Finance & Governance:-

"I would like to thank the Committee for the work it has undertaken in setting up the task and finish group chaired by Councillor Clifton, who looked at the various aspects and complexities of cyber security in a relatively short period of time.

In respect of the recommendations a) to g), they reflect a pragmatic and reasonable approach to supporting the Council's cyber security arrangements, so I am therefore supportive of taking the various activities forward in 2023/24.

Recommendations h) to j) of the Resources and Services Overview and Scrutiny Committee will be presented for consideration at Full Council on 2 March 2023 [Note: as set out above].

In respect of recommendation h), this reflects the position I have mentioned on a number of occasions over recent months. I appreciate the frustration that many Members have previously expressed, but I believe that the risk of continuing with the forwarding of emails to personal emails account is too great for various reasons, not least because of UK Data Protection legislation compliance, but also recognising freedom of information issues that have been highlighted by the ICO. Not only that, but the world of cyber security will keep evolving and there will be adverse consequences if we continued with current practices. We therefore need to remain alert to both current and future risks.

Furthermore, if a breach was to take place the Council would be potentially liable to hefty fines by the ICO.

I note that the following 4 options relating to how Members can access their Tendring District Council emails that were considered by the task and finish group:

1. *Use of council managed laptops only*
2. *All members be provided with a Council managed smart phone*
3. *Introduce a 'Bring Your Own Device' Service Framework*
4. *A Member web 'portal' app*

Whilst acknowledging the Committee's practical recommendation of the provision of Council managed smartphones, in striking a pragmatic balance along with recognising how Members are increasingly reliant upon flexible access to their emails to effectively undertake their role as a Councillor, I would be supportive of exploring Option 4 above in more detail as a possible alternative. Although the provision of a mobile phone would provide a practical solution, I understand the frustration of some members where they are juggling more than one email account to reflect their 'political' roles with that of a being a ward Councillor along with trying to undertaking that role efficiently. The responsibilities of Portfolio Holders giving direction and making decisions within their individual areas has also been taken into account.

In recognition of the above, I am therefore proposing that Officers also explore in more detail the option of a Members' 'portal' as a flexible way for Members' to continue to use their own devices to access their Tendring District email account.

Following the Council's consideration of the associated report at their meeting on 22 November 2022, the following resolution was agreed:

'the implementation of any and all changes required be planned for no later than 1st April 2023 in readiness for the commencement of the new Council, following the elections in 2023 and that the new Councillors be given the training'.

My proposed approach will have an impact on the above, which is addressed in my recommendations."

Having duly considered the recommendations submitted to Cabinet by the Resources & Services Overview and Scrutiny Committee, together with the response and recommendations of the Corporate Finance & Governance Portfolio Holder thereto, Cabinet:-

***"RESOLVED** that –*

a) the Resources and Services Overview and Scrutiny Committee be thanked for the work they have undertaken and specifically the Members who participated in the associated task and finish group, chaired by Councillor Clifton;
b) the Committee's recommendations a) to g) are agreed and Officers be requested to undertake the associated activities as soon as practicable in 2023/24 in consultation with the Portfolio Holder for Corporate Finance and Governance;

c) in respect of the Committee's recommendations h) to i), it is recommended to Full Council that:

   i) although it is recognised that the provision of mobile phones would provide a practical solution to enable Members to access their Tendring email accounts, Officers be requested to also explore the alternative option of a Members 'portal' before a final decision can be considered;

ii) subject to ci) above, a further report be presented to Cabinet as early as practicable in 2023/24 that sets out the outcome from the proposed review of the Members' 'portal' option and recommendations are presented back to a future meeting of Full Council;

iii) subject to ci) and cii) above, Full Council continues to acknowledge that the ongoing risk to the Council, in acting as Data Controller, could potentially be in breach of the Data Protection Act 2018 remains, whilst the auto-forwarding of Councillor emails practice continues; and

iv) whilst the work in ci) and cii) is ongoing, all Members elected in May 2023 are advised of this and the Council's Information Governance requirements through their induction programme."

A copy of the published reference report (and its appendices) from the Resources and Services Overview & Scrutiny Committee to the Cabinet meeting held on 17 February 2023, are attached as appendices to this report.

RECOMMENDATIONS

That Council considers the outcome of the enquiry into cyber security undertaken through the Resources and Services Overview and Scrutiny Committee and determines whether to adopt the following as recommended by Cabinet –

(a) although it is recognised that the provision of mobile phones would provide a practical solution to enable Members to access their Tendring email accounts, Officers be requested to also explore the alternative option of a Members' 'portal' before a final decision can be considered;

(b) subject to (a) above, a further report be presented to Cabinet as early as practicable in 2023/24 that sets out the outcome from the proposed review of the Members' 'portal' option and that Cabinet's recommendations arising therefrom are submitted to a future meeting of Full Council;

(c) subject to (a) and (b) above, Full Council continues to acknowledge the ongoing risk to the Council that, in acting as Data Controller, it could potentially be in breach of the Data Protection Act 2018 and that risk will remain whilst the auto-forwarding of Councillors' emails practice continues; and

(d) whilst the above work in (a) and (b) is ongoing, all Members elected in May 2023 be advised of this and of the Council's Information Governance requirements through their Members' induction programme.

BACKGROUND

Council will recall that, at its meeting held on 22 November 2022 (Minute 55 refers), it had considered a report of the Portfolio Holder for Corporate Finance and Governance, which presented to it an update on proposals for IT changes. That ongoing work was aimed at reaching an outcome whereby Members could undertake their role effectively, whilst ensuring that information held by the Council was safe, secure and compliant with relevant legislation. This work would also include looking at various different IT solutions and the

associated costs.

Council had been informed at that meeting that the Department of Levelling Up, Housing and Communities (DLUHC) had commenced local authority security resilience audits in 2021. In December 2021, the DLUHC 'Health Check' scan had identified this Council's auto-forwarding of emails practice as a risk and had recommended that the practice be phased out as soon as possible.

Members had also been informed that the original proposal to cease the auto-forwarding of emails had also emerged from an information governance / GDPR review undertaken by Internal Audit. The associated review, which supported that approach, had been undertaken in line with the Council's existing risk management processes and had included input from the Council's Data Protection Officer, Section 151 Officer, Internal Audit Manager and Senior Information Risk Owner (SIRO).

Members had been made further aware that Internal Audit's findings had been considered and agreed by the Audit Committee who, after considering the matter at its meeting held on 30 January 2020 (Minute 20 refers), had 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."

Subsequently, the March 2022 Corporate Risk Register had reported the need to cease the practice of auto-forwarding of Councillors' emails.

Council had been advised that the UK Data Protection legislation (6th Principle) required that information and data were processed in a manner that ensured 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 was the Data Controller and had legislative responsibility to ensure, and to evidence, that information was being managed and protected in accordance with the principles of the legislation.

It had been noted at that Council meeting that the original proposal of ceasing auto-forwarding of emails had been met with concern from some Members as they felt that it might curtail their ability to access information and fulfil their role. Therefore, the Portfolio Holder had 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.

Members had also been made aware that the Resources and Services Overview and Scrutiny Committee had included Cyber Security in their work programme. In consultation with the Chairman of that Committee, (Councillor M E Stephenson), it had been proposed that their remit be extended to include the issue of Members' access to their information and the alternative solutions available, mindful of the recommendations of the Audit Committee and the issues of confidentiality, Data Protection and cyber security.

In terms of the proposed review by the Resources and Services Overview and Scrutiny Committee, it had also been highlighted that the Council's existing adopted Risk Management Framework sought to address a number of key elements such as the

identification of risks, the analysis of those risks and whether they could be 'tolerated' or needed to be 'treated etc., with the latter including reviewing potential options. With that in mind, it had felt logical / pragmatic to structure the proposed review around those existing risk management principles, which formed part of the original work undertaken by Officers and the Audit Committee. That approach also complemented 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 had been considered at the first meeting of the Resources and Services Overview and Scrutiny Committee's Cyber Security Task and Finish Group held on 27 October 2022.

At its meeting held on 22 November 2022 and in respect of this matter, Full Council had decided, inter alia, that:-

"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 be mindful of the recommendations of the Audit Committee, Data Protection Act requirements and cyber security;"

BACKGROUND PAPERS FOR THE DECISION

Published Minutes of the meeting of the Full Council held on 22 November 2022.

Published Minutes of the meeting of the Cabinet held on 17 February 2023.

APPENDICES

Published Reference Report (and Appendices) (A.6) of the Resources and Services Overview & Scrutiny Committee for the meeting of the Cabinet held on 17 February 2023.