A.4 APPENDIX 1

CABINET

17 FEBRUARY 2023

REFERENCE REPORT FROM THE RESOURCES AND SERVICES OVERVIEW & SCRUTINY COMMITTEE

A.6 SCRUTINY OF CYBER SECURITY FOR THE COUNCIL

(Report prepared by Keith Durran and Keith Simmons)

BACKGROUND

At the meeting of the Resources and Services Overview and Scrutiny Committee (RSOSC) on 1 February 2023, it considered a report submitted by its own Task and Finish Group (T&FG) on Cyber Security.

In accordance with the RSOSC mandate the Cyber Security T&FG were tasked to:

1) To challenge/ better understand the cybersecurity risks, defences, and mitigations the Council has in place.

Following Full Council 22nd November 2022, the T&FG mandate was extended to additionally:

2) Review different proposals of Members' access to emails and the current practice of auto-forwarding to personal email accounts, in line with the Council's Risk Management Framework, and make recommendations to Cabinet and Council along with relevant costings.

During its first meeting the Cyber Security T&FG agreed to use the Department of Levelling Up Housing and Communities (DLUHC) Cyber Assessment Framework (CAF) document template as a self-assessment, auditing, and reporting framework template to review council cyber-security as referenced above.

The DLUHC CAF proved relevant to the review of Members' access to emails, auto-forwarding of council official business emails to personal devices and council data stored on personal devices as it includes a number of National Cyber Security Centre (NCSC) compliance statements covering: data security and understanding, data protection in transit across the UK network, data storage security, mobile device data security, media equipment sanitisation and disposal, secure device configuration.

CAF Explanatory Notes

The DLUHC Cyber Assessment Framework (CAF) provides the pragmatic basis to 'self-assess' the Council's own cyber security performance across the following activities:

1) Managing Cyber Security (organisational structures, policies, processes, understanding).
2) Protecting Against Cyber Attack - security measures to protect networks and systems.
3) Detecting Cyber Security Events ensuring effective security defences/ event detection.
4) Minimising The Impact of cyber security Incidents and their adverse impact.

The self-assessment CAF is a National Cyber Security Centre (NCSC) assessment document that has been a mandatory cyber-security 'readiness state audit' document for critical UK national infrastructure providers since 2021. During 2022 the CAF has become mandatory for every central government department and whilst CAF completion is currently

voluntary for local government DLUHC have repeatedly advised that it will become mandatory during 2023/24.

In this sense the CAF will replace the now defunct Public Services Network (PSN) IT Health Check annual audit/ certification process reporting local government cyber-security capabilities and fitness to remain securely connected and sharing data with central government Department of Works & Pensions (DWP). The reader should note that several council statutory service functions are completely reliant upon this connectivity, for example: Council Tax, Housing Benefit administration. Loss/ exclusion from central government connectivity would quickly stop these services from functioning.

With regards to the outcome, outlined recommendations were made by T&FG Members with due regard and consideration to:

- The Full Council background information report.
- All Members' subject matter comments received considered 23rd Jan'23.
- A newly published Information Commissioner's Office Freedom of Information (FOI) guidance note considered 23rd Jan'23.
- The four costed options provided and their respective financial, cyber-security and Member-user working practicality satisfaction and non-satisfaction implications considered 23rd Jan'23.
- A full copy of the Council's Cyber Assessment Framework (CAF). For simplicity, CAF compliance was reviewed utilising 'traffic light' red, amber and green representing non-compliance, improvements required and full compliance respectively.

Following CAF cyber-security compliance self-assessment, the T&FG identified that the council generally has robust cyber-security arrangements and working practices in place to manage, protect and safeguard the data that it holds to deliver both statutory and non-statutory services.

Its cyber-security event(s) detective arrangements utilising business industry-standard multi-vendor best-of-breed products are similarly robust and well managed.

However, the cyber-security self-analysis review also identified some areas of CAF cyber-security non-compliance, some areas where improvements could be made to further strengthen the Council's cyber-security.

The T&FG recommendations reflect improvements necessary to resolve CAF self-assessment key areas of non-compliance. Key areas considered by the T&FG were:

- **Recruitment and resourcing** key IT vacancies.
- **Risks unresolved** for prolonged periods.
- **Information retention** with data (including personal and sensitive data) stored for long periods of time with no clear business need.
- **Generic account used** or shared or default name accounts.
- **Training and understanding** individuals' contribution to essential cyber security.
- **Formal Adoption** of the new Cyber Incident Response Plan (CIRP).
- **Members' email auto-forwarding to personal/ mobile devices**, including; identification and data management, data security in transit, physical and/or technical security protection against unauthorised access, lack of knowledge around which

mobile devices hold data, allowing data to be stored on devices not managed by your organisation or to at least equivalent standard, lack of security on mobile devices, device disposal without data sanitisation, security builds that conform to your baseline or the latest known good configuration version.

RESOURCES AND SERVICES OVERVIEW & SCRUTINY COMMITTEE'S RECOMMENDATION(S) TO CABINET

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;

A.4 APPENDIX 1

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).**
PORTFOLIO HOLDER COMMENT(S) AND RECOMMENDATION(S) TO CABINET
PORTFOLIO HOLDER'S COMMENTS AND RECOMMENDATIONS TO CABINET: ***The response of the Corporate Finance and Governance Portfolio Holder, together with his recommendations to Cabinet, will be circulated to Members prior to the meeting.***