FINAL REPORT OF THE RESOURCES AND SERVICES OVERVIEW AND SCRUTINY COMMITTEE TASK & FINISH GROUP FOLLOWING ITS INQUIRY INTO:

THE COUNCILS CYBER SECURITY AND MEMBERS' E-MAIL AUTO-FORWARDING AND USE OF PERSONAL EMAIL ACCOUNTS

1 FEBRUARY 2023

TERMS OF REFERENCE OF THE TASK & FINISH GROUP

As part of its work programme for 2022/23, the Resources and Services Overview and Scrutiny Committee (RSOSC) established a Cyber Security Task and Finish Group to investigate and challenge the Council's cyber-security arrangements and preparedness. Full Council approved the proposed work programme for the RSOSC at Full Council 12 July 2022 (minute 29 refers) *"RESOLVED that Council – (a) approves the proposed work programmes for the Community Leadership and the Resources & Services Overview and Scrutiny Committees for the 2022/23 Municipal Year".*

For the purposes of this report Full Council agreed that the item forenquiry would be; *"Cyber Security for the Council. Looking at the threats, our approach to those threats and the future vulnerabilities. There was agreement that this might be a good subject for scrutiny."*

Resources and Services Overview and Scrutiny Committee 6 September 2022 (minute 23 refers) approved the membership of that T&Fgs. *"the Committee RESOLVED to approve the Membership/Chairman details in the list circulated at the meeting for Task and Finish groups identified and, consequently, authorised Task and Finish groups to commence the scrutiny enquires concerned as approved by Council".*

Subsequently, on 22 November 2022, Full Council considered an Information Governance Report that set out the background to the review of Members access to emails and the risks associated with forwarding emails to personal email addresses. This report is attached as *Appendix A*.It was resolved by Full Council 22 November 2022 (minute 55 refers) "RESOLVED that – *"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".*

THE AIMS AND OBJECTIVES OF THE INQUIRY

In accordance with Resources and Services Overview and Scrutiny Committee mandate the Cyber Security Task and Finish Group (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 (*see CAF explanatory notes*).

The DLUHC CAF proved relevant to the review of Members' access to emails, auto-forwarding of council official business emails to personal devices and 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 a number of 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.

MEMBERSHIP OF THE TASK & FINISH GROUP

Membership of the Task and Finish Group (T&FG) was as follows;

Cllr. Paul Clifton (Chair)	Cllr. Chris Amos	Cllr. Ann Wiggins
Cllr. Alan Coley	Cllr. Chris Griffiths	

OFFICER SUPPORT FOR THE TASK & FINISH GROUP

Officers providing technical, financial, legal and/or administrative support to the Group were as follows;

Richard Barrett – Assist. Director Finance and IT
John Higgins – Head of Digital & Assurance Services
Sam Wright – Cyber-security & Systems Support Manager

Keith Durran – Committee Services Officer
Lisa Hastings – Deputy Chief Executive & Monitoring Officer (Attended 23/01/23 meeting)

Non-attendee technical, information governance and CAF review support was additionally provided by;

Dan Pobjoy - Digital Operations Manager
Judy Barker - Information Governance & IT Services Manager and nominated Council Data Protection Officer.
Dr. Rupert Ogilvie – Specialist Consultant, Intergence Systems Ltd.

INVITEES AND PARTICIPANTS

As previously outlined, having agreed to use the Department of Levelling Up Housing and Communities (DLUHC) Cyber Assessment Framework (CAF) document template as an audit and self-assessment reporting tool to review council cyber-security. The Council's CAF self-assessment completion was additionally supported in the 'back-office' by officers J.Barker and D.Pobjoy together with specialist consultant Dr. R. Ogilvie.

At the 22nd November 2022 Full Council meeting considering the Information Governance Report setting out the background to the review of Members access to emails and the risks associated with forwarding emails to personal email addresses, Members were 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 Group to take into consideration. A small number of Members responded.

The Member comments received along with key points are set out in *Appendix B*. As requested, the Monitoring Officer has provided her responses and included a newly published Guidance Note produced by the Information Commissioner's Officer (ICO) on the applicability of the Freedom of Information Act 2000 to official information held in private email accounts. The Note clearly sets out the position that where information is held relating to local authority business in a Councillor's private email account this may be subject to the FOIA and is included as *Appendix C*.

EXPECTED OUTCOME(S) OF THE INQUIRY

In accordance with the Resources and Services Overview and Scrutiny work programme adopted by full council the value of the enquiry was; *"To challenge/ better understand the cybersecurity risks, defences and mitigations the council has in place."*

As previously outlined, the T&FG elected to adopt the DLUHC CAF self-assessment document as a means to self-assess and record the council's cyber-security strengths and weaknesses and make recommendation reference identified areas requiring improvement.

When additionally mandated by Full Council to consider different proposals for Members' access to emails, auto-forwarding in line with the council's risk management framework and consider costed options, this became a second and important point of T&FG discussion/ consideration with the resultant recommendation to Resources and Services Overview and Scrutiny Committee, Cabinet and Full Council.

ACTUAL OUTCOME(S) OF THE INQUIRY

With regards to the expected outcomes previously outlined recommendations were made by T&FG Members with due regard and consideration to;

- **Appendix A** - the Full Council background information report.
- **Appendix B** - all Member's subject-matter comments received considered 23rd Jan'23.
- **Appendix C** - a newly published Information Commissioner's Office Freedom of Information (FOI) guidance note considered 23rd Jan'23.
- **Appendix D** - 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.
- **Appendix E** - 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 rerspectively.
- **Appendix F** - for completeness, this report also includes a copy of the council's new Cyber Incident Response Plan (CIRP) which the T&FG recommends for adoption.

Note: All of the above documentation is included as appendices to this report

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-complaince. 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.

RECOMMENDATION(S)

The T&FG recommendation(s) to the Resources and Services Overview and Scrutiny Committee and Cabinet in respect of Cyber Assessment Framework (CAF) cyber-security non-compliance that;

a) **As soon as is possible the Human Resources and Council Tax Committee with appropriate officers look at the salary(s) being offered for the advertised and unfilled senior IT posts and including cyber security senior technical positions.**

b) **By 31/03/23 a Member & Officer 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) **By 31/07/23 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) **By 31/05/23 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) **Commencing no later than May 2023 following the election of the New Administration Cyber Security and Information Governance training for all members after every election and for staff in their inductions with periodic refresher training for both be made mandatory.**

f) **As soon as possible in consultation with 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) **As soon as possible the new Cyber Incident Response Plan (CIRP) included as Appendix F to this report be adopted.**

In reviewing the different options of Members' access to emails, reflecting the Council's Risk Management Framework, the recommendations to Full Council that the T&FG are submitting to the Resources and Services Overview and Scrutiny Committee and onwards to Cabinet are;

h) **That post-May 2023 local elections under the New Administration, that the Member practice of auto-forwarding of emails be ceased; and**

i) **that subject to the associated funding of £8,000 being identified that the preferred Option 2 (*Appendix D refers*) - 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 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 will be asked to fund the cost from allowances (circa two hundred pounds per annum).

CHRONOLOGY

- 12th July Full Council set the initial scope for the Cyber Security Task & Finish Group.
- 27th October 2022 first meeting of the Cyber Security Task & Finish Group
- 8th November 2022 second meeting of the Cyber Security Task & Finish Group.
- 22nd November 2022 Full Council considers the report of Deputy Leader & Portfolio Holder for Finance and Corporate Services Information Governance report reporting an update on proposals for IT changes and including consideration of different proposals for Members' access to emails.
- 8th December 2022 third meeting of the Cyber Security Task & Finish Group.
- 23rd January 2023 fourth and final meeting of the Cyber Security Task & Finish Group.
- 1st February 2023 Cyber Security Task & Finish Group report and recommendations to the Resources and Services Overview and Scrutiny Committee and onwards to Cabinet and Full Council.

DETAILED FINDINGS OF THE INQUIRY

It has always been fully acknowledged that Members need to be provided with information that allows them to fulfill their councillor duties, with any proposals put forward to date reflecting best practice and risk rather than a legal obligation or otherwise.

One of the key Member points raised related to the legal context of ceasing the auto-forwarding of emails. As highlighted in *Appendix B*, from a legislative perspective the UK General Data Protection Regulation (GDPR), particularly Article 5, Paragraph 1(f), requires personal data to be processed in a manner that ensures appropriate security of the personal data. The Council is unable to demonstrate compliance in this regard where the forwarding of emails is to a personal email account, which is outside of the control and management of the Council.

The published Information Commissioner's Office (ICO) guidance note (*Appendix C*) relating to official information held in private email accounts is intended to clarify the legal status under FOIA of information relating to the business of a public authority held in private email accounts, and other media formats and confirms that information held in non-work personal email accounts (e.g. Hotmail, Yahoo and Gmail) may be subject to FOIA if it relates to the official business of the public authority.

In addition to the request for comments mentioned previously, at the meeting of Full Council on 22 November 2022 Officers were asked to explore opportunities / options relating to Member's access to emails given the various issue raised. Although this piece of work had already been largely undertaken as part of previous activities, it has been revisited following this recent request by Members. *Appendix D* sets out this review in more detail, which includes the following 4 main options:

OPTION 1 - Restrict access to the Council's network / systems to only those devices owned and managed by the Council.

This represents the basis for the original recommendation of ceasing the forwarding of emails to personal devices reflects the existing arrangements where laptops were provided to all 48 Members along with mobile phones issued to specific members. However, it was noted via the discussions at Full Council on 22 November 2022 that some Members needed to continue using personal IT devices and especially personal mobile phones to react quickly to emails from residents, fellow members, officers and partner organisations.

Legally and constitutionally, only the Leader and Cabinet are Members who have the authority to make decisions urgently / individually, which reflects the issuing of mobile phones to specific Members as highlighted above.

OPTION 2 - Council owned / managed mobile phones issued to Members who request one (in addition to OPTION 1).

This option would meet the needs expressed by some Members to react quickly to emails from residents, fellow members, officers and partner organisations. Similarly, it accords with officer recommendations to optimise cyber-security through the use of council-managed-devices only protected within the council's cyber-security domain. Subject to how these devices are funded there may be additional cost implications.

OPTION 3 – Members continue to use their own personal devices but the Council installs and manages software on those devices.

This option meets the needs expressed by Members BUT to meet NCSC cyber-security standards will require loading council protective software on personal devices. This is known as 'Bring Your Own Device, or BYOD. Loading of council cyber-security management software onto Member's personal device(s) may be unpopular and/ or seen as invasive by some individuals, and there is a risk of outright refusal. Additionally, with the myriad of different devices and applications used by Members it is not possible to guarantee that faults and security/ personal application incompatibility issues won't occur nor possible loss of personal data held on devices e.g. photos.

There will be a requirement for additional council IT technical and administrative resources to adequately support this option with resultant additional and unbudgeted costs.

OPTION 4 – Members continue to use their own personal devices and access systems / emails via a web based Member 'Portal'

Again, this option meets the needs expressed by Members but increases instead of reduces the attack vectors available to cyber-criminals and therefore increases the council's risk of cyber-attack (bearing in mind that the council is notably already the third most attacked organisation in the East of England). The portal would need to be configured on a *"one size fits all basis"* so the user-experience quality would differ between different devices and could not be individually tailored.

To deploy and maintain this option securely will require additional specialist cyber-security resources and council IT technical and administrative resources and incur additional licensing costs. All of which means that adoption will result in additional and unbudgeted costs.

As set out in *Appendix D,* in determining a way forward a balance needs to be made between cost, convenience, compliance with data protection requirements, resources and the risk of a cyber-attack, with a summary of some of the key points as follows:

- Meeting Member's home-based and mobile working requirements
- User satisfaction

- Cost vs. risk
- Strength of the Council's Cyber Security position
- Members information governance arrangements
- Complexity and resources requirement
- Adequacy of the management of risk

The T&FG detailed findings together with the relevant CAF references and their recommended remediation actions are as follows and reflected in the recommendations set out previously;

Cyber Assessment Framework Module	Issue	Recommendation(s)
Managing Security Risk and Detecting Cyber Security Events: CAF Ref A1.b Roles and Responsibilities- *"Your organisation has established roles and responsibilities for the security of networks and information systems ."* AND CAF REF: C1.e Monitoring Tools and Skills AND C2.b Proactive Attack Discovery	Recruitment and resourcing	That the Human Resources and Council Tax Committee and/or appropriate officers look at the salary(s) being offered for the advertised and unfilled senior IT posts and including cyber security senior technical positions.
Managing Security Risk CAF Ref: A2.a Risk Management Process – *"Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities."*	Risks unresolved for long periods.	That a Member & Officer Cyber Security Group be established to periodically review the Council's cyber security performance against the CAF and/or emerging mandatory security improvements and requirements.
Managing Security Risk CAF Ref: A3.a Asset Management – *"Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy."*	Information retention management	That 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.
Managing Security Risk CAF Ref: B2.c Privileged User Management – *"Privileged user access to your essential function is via generic, shared or default name accounts."*	Generic Accounts	That Individual (non-generic) account access technologies be costed for accessing TDC terminals in locations such as leisure centres were numerous users sharing a terminal due to a retail environment operational need.
Managing Security Risk and Protecting Against Cyber Attack CAF Ref: B6.a Cyber Security Culture – *"You develop and pursue a positive cyber security culture."* And *"All people in your organisation understand the contribution they make to the essential function's cyber security."*	Training and understanding	That Cyber Security and Information Governance training for all members after every election and for staff in their inductions with periodic refresher training for both be made mandatory.
Protecting Against Cyber Attack AND	Training and understanding:	In consultation with the Council's Monitoring Officer, to review

T&FG Member comments/ disucssions		existing Member guidance and explore Member training opportunities as to what constitutes party political activities in the context of using a TDC email account.
Minimising The Impact of Cyber Security Incidents CAF Ref: D1.a Response Plan -" *You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios."*	Adoption of the new Cyber Incident Response Plan (CIRP).	That the new Cyber Incident Response Plan (CIRP) included as Appendix F to this report be adopted.

With reference to the recommendations regarding Members' access to emails, there are a number of relevant CAF references considered by the T&FG, as follows;

CAF Reference	**Compliance Statement Descriptive Text (See Note)**
CAF ref B3.a Understanding Data	*"You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the essential function. This also applies to third parties storing or accessing data important to the operation of essential functions."*
CAF ref B3.b Data in Transit	*"You have protected the transit of data important to the operation of the essential function. This includes the transfer of data to third parties."*
CAF ref B3.c Stored Data	*"You have protected stored data important to the operation of the essential function."*
CAF ref B3.d Mobile Data	"*You have protected data important to the operation of the essential function on mobile devices."*
CAF ref B3.e Media Equipment Sanitisation	"*You appropriately sanitise media and equipment holding data important to the operation of the essential function."*
B4.b Secure Configuration	"*You securely configure the network and information systems that support the operation of essential functions."*

Note: To achieve CAF compliance the Council is required to confirm that the above statements reflect the Counci's current position which we are unable to do given the current Member auto-forwarding of emails arrangements.

BACKGROUND PAPERS AND PUBLISHED REFERENCE MATERIAL

Background papers and reference materials are included as appendices A-F as outlined below.

APPENDICES

Appendix A: The 22nd November 2022 Full Council background information report .

Appendix B: All Member's subject-matter comments received with the Monitoring Officer response(s).

Appendix C: A newly published Information Commissioner's Office Freedom of Information (FOI) guidance note in relation to emails stored on personal devices

Appendix D: The four costed options provided and their respective financial, cyber-security and Member-user working practicality satisfaction and non-satisfaction implications.
Appendix E: A copy of the council's Cyber Assessment Framework (CAF).

Appendix F: A copy of the council's new Cyber Incident Response Plan (CIRP) which the T&FG recommends for adoption.

REPORT CONTACT OFFICER(S)	
Name:	Richard Barrett
Job Title:	Assistant Director Finance & IT
Email/Telephone	rbarrett@tendringdc.gov.uk Tel 01255686521

Name	John Higgins
Job Title	Head of Digital & Assurance Services
Email/Telephone	jhiggins@tendringdc.gov.uk Tel 01255686339