APPENDIX D

Members Access to Emails – Opportunities / Options

Option / Description	Financial Implications	Positive Considerations	Negative Considerations
OPTION ONE ▪ Each Member is provided with a Council-managed Laptop Only. ▪ Cabinet Members are also provided with Council-managed mobile telephone. ▪ Council systems/ communications / emails are only accessible by a council-managed devices.	Already budgeted	**Optimum Data Protection and Full UK Data Protection Legislative Compliance** in terms of transparency, security protective measures and data destruction that can be evidenced by the council as the Data Controller for all council official business purposes. **Member's personal devices would not be subject to council related Freedom Of Information (FOI)** requests nor Information Commissioner's Office investigation as Members have no council official business information on their personal device(s). **Strongest Possible/ Least Vulnerable Cyber Security Position -** a managed device is the safest and strongest cyber-security position that the council can realistically adopt in consideration to; 1) The ever increasing risk of a major cyber-security attack and subsequent loss of services, multi-million pound financial cost of recovery, loss of reputation, risk of harm to residents and particularly vulnerable residents and potentially loss-of-life. 2) It accords with the cyber-security industry direction of travel towards a *'zero trust model'* where each user, each device security-health/ integrity and access to every service(s) is constantly being verified by automated cyber-security system 'handshakes' through security and authorisation policies. *NOTE: The Zero-trust model, or zero trust network access (ZTNA), Introduction to Zero*	**User Dissatisfaction** as some users may prefer to use a personal device(s) that they feel most comfortable with. **User Dissatisfaction** as does not facilitate some member's requirements to work whilst working remotely along with delays in responding to emails etc.

		Trust - NCSC.GOV.UK or Why the time has come for Zero-Trust model of cybersecurity | World Economic Forum (weforum.org) direction of travel is increasingly being adopted by every security aware organisations including many local authorities where users are distributed on different networks e.g. home and office. **Cyber-security Management/ Risk Control.** This model removes cyber-security protective decisions and actions away from 'the individual' through security update automation, management and robust enforcement of cyber-security standards and best-practice. **Council IT Servicedesk support** during operational hours. **Council IT Standard Model** option with no additional council resourcing requirements in terms of officer resource, training and support. All officers work in this manner using the same standard specification laptop/ smartphones.	
OPTION TWO ▪ As per 'Option One' But additionally that; ▪ All Members to be offered a standard model council managed smartphone to use and access emails whilst mobile.	Additional revenue (ongoing) corporate council costs of **£8,000k** per annum (for 40 members) Alternatively Members meet the on-going cost of the smartphone from their Member's Allowance (£200 per annum)	As Option One in addition to: **Provides an alternative device to support Member's working remotely**	**User Dissatisfaction** as some users may prefer to use a personal device(s) that they feel most comfortable with. Also the TDC supplied device would not necessarily be the latest Samsung device. **User Dissatisfaction** as users may be unwilling to carry two mobile phones i.e. their new TDC phone and a personal phone. **If the cost is not met from Member's own allowances, then there would be an additional cost that would have to be met from within the financial forecast.**

OPTION THREE Members' continue to use their own personal devices e.g. laptops / tablets / smartphones of choice but managed within a Bring Your Own Device (BYOD) Service Framework This framework would require the installation of Mobile Device Management (MDM) security software onto any personal devices used. *Notes: BYOD services are designed to offer the same level of IT security to corporate data (only) as a managed device. Due to this the device is locked down with high level encryption. The council cannot see your personal information. When you enrol a device, you give us permission to view certain pieces of information on your device only, such as device model and serial number and security settings.*	Estimated One-off setup costs of **£22,000.** Estimated On-Going Revenue costs of potentially up to **£50k to £70k** per annum.	**Meets ALL Member's home-based and working mobile requirements** accessing council official business emails from any personal device(s). **Strong Microsoft Cyber Security position** that meets National Cyber Security Centre (NCSC) and Department of Levelling Up and Housing Communities (DLUHC) current minimum standards. *NOTE: Members should consider the National Cyber Security Centre (NCSC) 'Bring Your Own Device (BYOD)' guidance text included below.* Only provides some of the information governance and cyber-security protective measures as set out in Option one and Two above.	Only provides some of the information governance and cyber-security protective measures e.g. **Limited data protection and UK data protection legislative compliance.** Confidentiality is not guaranteed and remains the responsibility of each Member. Similarly the issue of auto-forwarding and legislative transparency is not resolved. **Limited Council IT Servicedesk support** during operational hours. **Member's personal devices would potentially remain subject** to council-related Freedom Of Information (FOI) requests and Information Commissioner's Office investigation as they will hold council official-business information. **Not all users may agree to have Council MDM software loaded and updated on their personal device(s) so this may only provide a partial solution.** **User Dissatisfaction -** With members accessing services through different personal devices the user-experience cannot be guaranteed and there is a risk that it may impact on the functioning of personal applications which cannot be supported by the in-house IT team, which could include the loss of personal data. **It is relatively expensive to implement and the additional cost would have to be met from within the financial forecast.** Costs include: • licensing costs • technical / admin support costs **Not necessary a long term solution e.g.** NCSC/ DLUHC cyber-security hardening may necessitate additional software controls being added to Member's

			personal device(s) to continue access or it becomes an option that is no longer deemed to reflect best practice. **** Please also see the note at the end of this table that sets out the NCSC view on such options.***
OPTION FOUR **A Member Web-Portal App** accessible by all Member's personal devices from anywhere in the UK (Would negate the need for auto-forwarding of emails)	Estimated one-off setup costs of **£16,000.** Estimated On-going Revenue costs of up to £70k per annum.	**Option Three provides most of the information governance and cyber-security protective measures as follows;** Strong data protection (however, confidentiality is not guaranteed and remains the responsibility of each Member. Full UK data protection legislative compliance. Member's personal devices would not be subject to council related Freedom Of Information (FOI) requests nor Information Commissioner's Office investigation. **Council IT Servicedesk support during operational hours.** **Meets Member's home-based and working mobile requirements** accessing council official business emails from any personal device(s). **Strong Microsoft Cyber Security position** that meets National Cyber Security Centre (NCSC) and Department of Levelling Up and Housing Communities (DLUHC) current minimum standards.	**Reduced Cyber Security Strength** - A Members' Web Portal cannot provide the full protection of a fully council-managed device only solution. It also opens another 'attack vector' for cyber-aggressors to attack (industry best-practice seeks to minimise not expand attack-vectors). Similarly, a ZTNA model cannot be fully achieved. **Cyber-Security Complexity And Resourcing** - It further complicates the council's cyber-security arrangements requiring additional management, monitoring, support and training resources. **User Dissatisfaction** - each Member would have to agree to have a Multi-Factor-Authenticator App loaded onto their personal device(s) to access the service. **Not necessary a long term solution e.g.** NCSC/ DLUHC cyber-security hardening may necessitate additional software controls being added to Member's personal device(s) to continue access or it becomes an option that is no longer deemed to reflect best practice. **User Dissatisfaction** – the Web Portal will have to provide a standard 'look and feel' regardless of Member's personal device choice(s) so there may be differing views on the 'standard user experience' it offers. **Cyber-security Management/ Risk Control** remains the responsibility of each Member with some

			Member's devices remaining unpatched with weak passwords leaving them open to a successful cyber-attack and in turn hostile-use of their device(s) to attack the council. **It is relatively expensive to implement and the additional cost would have to be met from within the financial forecast.** Costs include: • licensing costs • technical / admin support costs

*The use of personal devices for government official business is permitted - with reference to the use of personal mobile phones/ computers the National Cyber Security Centre (NCSC) 'Bring Your Own Device (BYOD)' guidance states: *"No BYOD deployment will protect corporate data as effectively as corporately managed devices, so consider what would happen if the services you intend to expose were compromised and the business impact it would cause. … it comes with a conflicting set of security risks and challenges. … You should understand what your IT department will be able to cope with. Supporting all the devices that can be used for BYOD will almost certainly prove problematic. … Usability will be a focus for the device owners themselves, desiring no disruption of their usual experience of a device. They will also likely have concerns over the privacy of their personal data, the impact of which will vary depending on the degrees of corporate control you intend to implement. … Because the organisation will have less control and visibility of a user's personal device than of a corporately owned and managed one, BYOD faces greater security risks."* https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device