A.6 APPENDIX A

FULL COUNCIL

22 NOVEMBER 2022

REPORT OF DEPUTY LEADER & PORTFOLIO HOLDER FOR FINANCE AND CORPORATE SERVICES

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 group to take into consideration. This can be done via email to Democratic Services

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 3 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.

Comments Received from Members Including Additional Comments / Response

Comments Received	Additional Comments / Response
Councillors are independently elected individuals, they are not employees of the council - as such they are entitled to be provided with information that allows them to fulfill that duty. For clarification, if they were employees and subject to the organisations employee policy then they would also be entitled to pensions, holiday and sick - which they are not.	Agreed. This was acknowledged in the report considered by Full Council on 22 November 2022. The Monitoring Officer has responded that Tendring District Council comprises of 48 members, otherwise called Councillors. One or more Councillors will be elected by the voters in Wards in accordance with a scheme drawn up by the Local Government Boundary Commission for England, and approved by the Secretary of State. Once elected Members form part of the Council, their roles are different to employees but collectively form the Council and become part of the public authority environment and framework in which local government sits. Article 2.04 of the Council's Constitution states that: • Councillors will at all times observe the Members' Code of Conduct and protocols set out in Part 6 of this Constitution. • Councillors are also expected to comply with the requirements of any risk assessments issued by the Council in performance of their functions
They have the right to have that information sent to their own personal devices in order to fulfill their duties - This is a protected right under protocol 1, Article 1 HRA 1998.	Protocol 1, Article 1 protects your right to enjoy your property peacefully - *every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.* Property can include things like land, houses, objects you own, shares, licences, leases, patents, money, pensions and certain types of welfare benefits. A public authority cannot

	take away your property, or place restrictions on its use, without very good reason. This right applies to companies as well as individuals. The Monitoring Officer has responded that it's unclear how the right to own a personal device is impacted upon by this subject area. It is not intending to take away the property, or place restrictions on its use, the Council is considering ceasing automatic forwarding to a personal device, from its own systems. However, the right is not an absolute right and can be interfered with, upon justification, such as compliance with legal requirements. 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. As part of previous considerations, the recommendation to stop the forwarding of emails has always been based on risk / best practice and compliance. Please see comments elsewhere in this report / appendices that set out the risks of members using their own personal devices. It is also important to highlight that the continuation of allowing the forwarding of emails to personal devices may prevent the Council connecting to the Government's network as this may be deemed a 'failure' against the associated Cyber Assessment Framework (CAF) that is currently being trialled / piloted.
It is down to the Council to make sure no information is shared that would constitute a breach of DPA - it doesn't matter if it is on council equipment or not, they send it to an independent person not in the organisation so have to comply every time an email is	As highlighted in the report to Full Council on 22 November 2022 the UK GDPR 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. The Council is 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.

sent. Those emails then being forwarded is irrelevant to this legal requirement.	The Monitoring Officer has responded, it is important to recognise is the difference between the Council, as Data Controller auto-forwarding, without an assessment of the content of the email, and an individual forwarding manually with intention knowing the content of the email. **However, potential alternative options are set out in Appendix D, that may address the wider point.**
Officers need to comply because the Council is the data controller for the data they use and they do handle sensitive personal data - councillors generally do not and are their own data controller.	Please see comment above. The Monitoring Officer has responded the proposed recommended action of ceasing auto-forwarding emails was to ensure the Council did not breach the requirements of the Data Protection Act 2018. Paragraphs 3.3 and 3.8 of the Members' Code of Conduct state that Members: 3.3 must not disclose confidential information or information which should reasonably be regarded as being of a confidential nature, without the express consent of a person authorised to give such consent, or unless required by law to do so. 3.8 Must observe the law The Council received advice and recommended action from the Audit Committee, Portfolio Holder for Corporate Finance and Governance and those Officers responsible for Audit, IT and Governance on a way forward to protect the Council, as Data Controller and mitigating Cyber Security risks. If Members wish to retain auto-forwarding of emails, they are the decision makers setting Policy in this regard on behalf of the Council, as Data Controller.
Most information in emails is in fact in the public domain anyway.	Unfortunately, this is more often not the case. Personal information is included in various emails from the public to Members, which can also be 'repeated' as part of longer email 'strings' if forwarded on more than once. Members are provided with considerable amount

	of confidential information.
Forwarding emails is not a major cyber security issue - it is a perfectly normal and safe activity which has been available for many decades, which is why it's an available function.	Similar to the above, this is no longer the case, which has been highlighted by a recent security incident. As previously discussed, the auto-forwarding of emails can easily create additional points of attack for cyber attackers who can for example 'harvest' information that can be used in various activities, such as social engineering and "Spear phishing" and "Whaling" (digitally enabled fraud through social engineering).
The council system is already overly restrictive with many residents emails being sent to spam or they get emails back saying that their email is undeliverable - councillors need to be able to receive emails from outside the council unhindered.	This has also been an issue raised directly by the Task and Finish Group with recommendations set out in the main body of the report. In the event that the forwarding of emails was ceased, Members can still use their personal email accounts to receive emails from the public for example. They may then wish to forward them onto their TDC account.
Government Department's opinion on the law is no more relevant than anyone else's - they do not make or interpret law and have no powers to enforce their opinion - nothing the background info is relevant.	Please see earlier response. The Monitoring Officer has responded that the information contained within the Background Section of the Report to Full Council in November, included occasions that matters related to this subject has been considered by Members in various meetings, including the Audit Committee and the Resources and Services Overview and Scrutiny Committee. With regards to not following the relevant Government's department for Local Government (currently DLUHC) guidance and policy, this will have an adverse and detrimental impact on the Council's reputation and access information held on the Government's network and to external funding streams to deliver projects for the local area. As the UK's technical authority for cyber security, the National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF) to support the UK's implementation of the European Union's Network and Information Systems (NIS) Directive in 2018.

	It is mandatory for critical infrastructure providers to achieve CAF latest NCSC cyber-security compliance standards. Similarly during 2022/23 central government departments are working towards CAF compliance. With this in mind, the new **Government Cyber Security Strategy** set out plans to adopt the CAF as the assurance framework for government, providing a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed. The strategy explains how the government will ensure all public sector organisations will be resilient to cyber threats and sets out plans to ensure that the government assesses its cyber resilience consistently and comparably. This includes adopting the NCSC's CAF as a standard way of assessing cyber risk. Whilst CAF compliance is today voluntary for local government, DLUHC have advised that during 2023/24 they are undertaking a number of local government voluntary compliance audits and Tendring is engaged in this process from a feedback perspective. It remains DLUHC's declared intention to mandate local authority CAF completion and compliance submission review and audit annually. This future CAF compliance regime will in essence replace the now defunct annual Public Services Network (PSN) Code of Connection cyber-security certification compliance review. CAF compliance failure and the possibility of disconnection from the PSN (which connects and facilitates data sharing between the council and government departments) would significantly affect and possibly even stop the council's ability to deliver key statutory services.
There is nothing illegal (breach of DPA) in forwarding information to independent elected people that are not part of the organisation and handle their own data - that's the only legal position that matters.	Please see earlier response. Similarly ***Appendix C***, the ICO's note outlining legal responsibilities around the use of personal email accounts and Freedom Of Information (FOI) enquiries is additionally relevant.
The practice of auto-forwarding emails MUST stop, regardless of any arguments put forward by councillors.	The ceasing of the forwarding of emails would reflect best practise. Options to address the associated risks are set out in **Appendix D.**

I think it was mentioned at an AMB that we are the only Council in Essex to allow it.	
Local Authorities are now experiencing requests for information, emails etc. that are held on 'private devices', where they relate to Council business. This could become an issue going forward, and despite it being said that Councillors are not subject to FOIA, they are if they are conducting Council business from a private device. This is something that might need to be clarified with our FOIA person.	Councillors would not be subject to FOI on their personal emails / devices if it did not relate to Council business, but once they have chosen to use their personal emails to correspond with the Council and act on behalf of the Council, a search of their emails may be necessary to respond to such requests. This is likely to be a matter that is eventually determined by the ICO going forward in the event that a requestor is unsatisfied with a Local Authorities response to withhold such information. Members who continue to have auto-forwarding in place, are in effect accepting that their personal email accounts are being used for Council business. The Monitoring Officer has responded that the Information Commissioner's Office has produced a Guidance Note on the topic of Freedom of Information Act 2000 to official information held in private email accounts and is attached as Annex Bi. The Note is helpful as it refers to a Councillor holding information relating to local authority business in her/her private email account on behalf of the local authority. It would be useful for this note to be circulated to all Members for information.
Council business should not be being done between Councillors on private email, look what happens at government level! There is, in my opinion, no valid reason that anyone needs to have their emails forwarded. Just because it has been done in the past, does not mean that it is still the right thing to be done, as has been highlighted by officers, government, and our own Audit Committee in the last few months	This reflects best practice - please see comments.

Maybe officers should start to refuse to act on any emails that come in from councillors private email addresses. Maybe that could be a recommendation by your Task and Finish Group.	This is covered in previous recommendations that council business should be undertaken on council-managed equipment. Should an email be received from a member's personal email account then officers should routinely respond to their TDC official address.
Whilst I think the IT team do an excellent job I still think there are areas where the use of personal equipment is not addressed. I understand that some councillors are not happy with having to use council equipment as they are use to their own but I think there are ways the council can look at facilitating this if everyone has Microsoft office on their own computers or laptops with inbuilt security. Has the option of using webmail rather than forwarding of emails been used? I have another outlook account accessed this way that I can pick up on my phone as well and I am asked to sign in every 7 days with random requests to verify my id via a code sent to my phone.	Potential alternative options are set out in **Appendix C.**
I do not think that emails addressed to councillors should be automatically directed to their personal accounts – whilst I doubt there is anything amiss happening I don't think the council should be in a position that there could be. If the use of personal email addresses/equipment is to continue then I	Please see comments above.

feel there should be some sort of signed agreement to mitigate risk.	
There needs to be compulsory initial training for all councillors in the first instance, then those that do/don't need more can be identified?	Training for Councillors is already in place. However further recommendations from the Task and Finish Group are set out in the main body of the report.

Official information held in private email accounts

Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) gives rights of public access to information held by public authorities.

An overview of the main provisions of FOIA can be found in the Guide to Freedom of Information.

This is part of a series of guidance, which goes into more detail than the Guide to FOIA, to help you as a public authority to fully understand your obligations, as well as promoting good practice.

This guidance is intended to clarify the legal status under FOIA of information relating to the business of a public authority held in private email accounts in particular, but also other media formats. This is an emerging area of FOIA compliance and so the guidance may be updated in due course.

This guidance does not deal with exemptions which might be applicable to information held in private email accounts, only whether it may be held for the purposes of FOIA.

Overview

- FOIA applies to official information held in private email accounts (and other media formats) when held on behalf of the public authority. Such information may be exempt and will not necessarily have to be disclosed.
- It may be necessary to request relevant individuals to search private email accounts in particular cases. The occasions when this will be necessary are expected to be rare.
- Adherence to good records management practice should assist in managing risks associated with the use of private email accounts for public authority business purposes.

What FOIA says

Section 3 sets out the two legal principles by which it is established whether information is held for the purposes of FOIA.

> **3.**
> (2) For the purposes of this Act, information is held by a public authority if—
>
> (a) it is held by the authority, otherwise than on behalf of another person, or
>
> (b) it is held by another person on behalf of the authority.

Under section 3(2)(a) information will be held by the public authority for the purposes of FOIA if it is held to any extent for its own purposes. Only if information is held solely on behalf of another person will the public authority not hold it for the purposes of FOIA.

Section 3(2)(b) provides that in circumstances where information is held by another person on behalf of the public authority, the information is considered to be held by the authority for the purposes of FOIA. It is this sub-section that is of relevance to information held in personal email accounts.

The Commissioner's approach

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. All such information which is held by someone who has a direct, formal connection with the public authority is potentially subject to FOIA regardless of whether it is held in an official or private email account. If the information held in a private account amounts to public authority business it is very likely to be held on behalf of the public authority in accordance with section 3(2)(b).

This can apply to any public authority. For example, a Councillor may hold information relating to local authority business in his/her private email account on behalf of the local authority. The Commissioner is aware that the issue has also arisen in a central government context in relation to the use of non-work systems. There is a need to have a clear demarcation between political and departmental work. In the local government context, there is a

need to have a clear demarcation between Council business and work for individuals as their local representative.

Information in private email accounts that does not relate to the business of the public authority will not be subject to FOIA.

Situations where information legitimately requested under FOIA includes relevant information held on private email accounts will be rare. However, when a request for information is received, public authorities should consider all locations where relevant information may be held. This may include private email accounts.

The ICO recommends that, as a matter of good practice, public authorities establish procedures for dealing with such situations. These should outline the relevant factors to be taken into account in deciding whether it is necessary to ask someone to search their private email account for information which might fall within the scope of an FOI request the public authority has received. Relevant factors are likely to include:

- the focus of the request, indicated by the words used by the requester;
- the subject matter of the information which falls within the scope of the request;
- how the issues to which the request relates have been handled within the public authority;
- by whom and to whom was the information sent and in what capacity (e.g. public servant or political party member); and
- whether a private communication channel was used because no official channel was available at the time.

Where a public authority has decided that a relevant individual's personal email account may include information which falls within the scope of the request and which is not held elsewhere on the public authority's own system, it will need to ask that individual to search their account for any relevant information.

The enquiries made should be directed towards deciding whether any information which is so held was generated in the course of conducting the business of the public authority. If it was, it is likely to be within the scope of the request. It will therefore be held by the individual on behalf of the public authority for the purposes of FOIA.

Where members of staff or other relevant individuals have been asked to search private email accounts for requested information,

there should be a record of the action taken. The public authority will then be able to demonstrate, if required, that appropriate searches have been made in relation to a particular request. The Commissioner may need to see this in the event of a section 50 complaint arising from the handling of the request.

Relevant information in other forms

Although the main emphasis of this guidance is on information held in private email accounts, public authorities should be aware that it applies to information in other forms. The definition of information under FOIA is provided at section 84 and states that ""information" … means information recorded in any form". Therefore, official information recorded on mobile devices, including text messages on mobile phones, or in any other media, may also be considered to be held on behalf of the public authority in the circumstances outlined in this guidance. Again, this does not necessarily mean that such information will be disclosable, but, on receipt of a valid FOIA request, public authorities should consider all locations where the requested information may be found.

Concealment and deletion

Public authorities should also remind staff that deleting or concealing information with the intention of preventing its disclosure following receipt of a request is a criminal offence under section 77 of FOIA. For example, where information that is covered by a request is knowingly treated as not held because it is held in a private email account, this may count as concealment intended to prevent the disclosure of information, with the person concealing the information being liable to prosecution.

Records Management

The Lord Chancellor's Code of Practice under section 46 of FOIA stresses the importance, and benefits, of having good records management. As such, public authorities are strongly advised to use their records management policies to clarify the types of information that could be considered as records relating to the public authority's business. These policies should include clear advice to staff that recorded information held by individuals, regardless of the form in which it is held, and which relates to the business of the authority, is likely to be held on behalf of the authority and so subject to FOIA.

In order to avoid the complications of requesting searches of private email accounts, and other private media, records management policies should make clear that information on authority-related business should be recorded on the authority's record keeping systems in so far as reasonably practicable.

It is accepted, that in certain circumstances, it may be necessary to use private email for public authority business. There should be a policy which clearly states that in such cases an authority email address must be copied in to ensure the completeness of the authority's records. In this way, records management policies will make it easier for public authorities to determine whether information is held and to locate and retrieve it in response to requests. If the information is contained within the public authority's systems it can also be subject to consistently applied retention and destruction policies.

Other considerations

Additional guidance is also available if you need further information on:

- Records Management

⇒ see the Code of Practice under section 46
⇒ see our guidance on Section 46 Code of Practice – records management

- Holding information

⇒ see Information held by a public authority for the purposes of the FOI Act
⇒ see When is information caught by the FOI Act?

More information

This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information or data protection, please https://ico.org.uk/global/contact-us/

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 <u>not guaranteed</u> and remains the responsibility of each Member. Similarly the issue of auto-forwarding and legislative transparency <u>is not resolved.</u> **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 <u>the user-experience cannot be guaranteed</u> 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

DETECTING CYBER SECURITY EVENTS
The organisation monitors the security status of the networks and systems supporting the operation of essential functions in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true	
Data relating to the security and operation of your essential functions is not collected.	Data relating to the security and operation of some areas of your essential functions is collected but coverage is not comprehensive.	Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function (e.g. presence of malware, malicious emails, user policy violations).	
You do not confidently detect the presence or absence of Indicators of Compromise (IoCs) on your essential functions, such as known malicious command and control signatures (e.g. because applying the indicator is difficult or your logging data is not sufficiently detailed).	You easily detect the presence or absence of IoCs on your essential function, such as known malicious command and control signatures.	Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function.	
You are not able to audit the activities of users in relation to your essential function.	Some user monitoring is done, but not covering a fully agreed list of suspicious or undesirable behaviour.	You easily detect the presence or absence of IoCs on your essential functions, such as known malicious command and control signatures.	
You do not capture any traffic crossing your network boundary including as a minimum IP connections.	You monitor traffic crossing your network boundary (including IP address connections as a minimum).		

A.6 APPENDIX E

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true
It is possible for logging data to be easily edited or deleted by unauthorised users or malicious attackers.	Only authorised staff can view logging data for investigations.	The integrity of logging data is protected, or any modification is detected and attributed.
There is no controlled list of who can view and query logging information.	Privileged users can view logging information.	The logging architecture has mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify. This includes protecting the function itself, and the data within it.
There is no monitoring of the access to logging data.	There is some monitoring of access to logging data (e.g. copying, deleting or modification, or even viewing.)	Log data analysis and normalisation is only performed on copies of the data keeping the master copy unaltered.
There is no policy for accessing logging data.		Logging datasets are synchronised, using an accurate common time source, so separate datasets can be correlated in different ways.
Logging is not synchronised, using an accurate common time source.		Access to logging data is limited to those with business need and no others.
		All actions involving all logging data (e.g. copying, deleting or modification, or even viewing) can be traced back to a unique user.
		Legitimate reasons for accessing logging data are given in use policies.

A.6 APPENDIX E

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true	
Alerts from third party security software is not investigated e.g. Anti-Virus (AV) providers.	Alerts from third party security software are investigated, and action taken.	Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.	
Logs are distributed across devices with no easy way to access them other than manual login or physical action.	Some, but not all, logging datasets can be easily queried with search tools to aid investigations.	A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.	
The resolution of alerts to a network asset or system is not performed.	The resolution of alerts to a network asset or system is performed regularly.	Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.	
Security alerts relating to essential functions are not prioritised.	Security alerts relating to some essential functions are prioritised.	Security alerts relating to all essential functions are prioritised and this information is used to support incident management.	
Logs are reviewed infrequently.	Logs are reviewed at regular intervals.	Logs are reviewed almost continuously, in real time.	
		Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.	

Not achieved - At least one of the following statements is true	Partially achieved - All of the following statements are true	Achieved - All the following statements are true	

Your organisation has no sources of threat intelligence.	Your organisation uses some threat intelligence services, but you don't necessarily choose sources or providers specifically because of your business needs, or specific threats in your sector (e.g. sector-based infoshare, ICS software vendors, anti-virus providers, specialist threat intel firms, special interest groups).	You have selected threat intelligence feeds using risk-based and threat-informed decisions based on your business needs and sector (e.g. vendor reporting and patching, strong anti-virus providers, sector and community-based infoshare, special interest groups).	
You do not apply updates in a timely way, after receiving them. (e.g. AV signature updates, other threat signatures or Indicators of Compromise (IoCs).	You receive updates for all your signature based protective technologies (e.g. AV, IDS).	You apply all new signatures and IoCs within a reasonable (risk-based) time of receiving them.	
You do not receive signature updates for all protective technologies such as AV and IDS or other software in use.	You apply some updates, signatures and IoCs in a timely way.	You receive signature updates for all your protective technologies (e.g. AV, IDS).	
You do not evaluate the usefulness of your threat intelligence or share feedback with providers or other users.	You know how effective your threat intelligence is (e.g. by tracking how threat intelligence helps you identify security problems).	You track the effectiveness of your intelligence feeds and actively share feedback on the usefulness of IoCs and any other indicators with the threat community (e.g. sector partners, threat intelligence providers, government agencies).	

Not achieved - At least one of the following statements is true	**Partially achieved - All of the following statements are true**	**Achieved - All the following statements are true**	
There are no staff who perform a monitoring function.	Monitoring staff have some investigative skills and a basic understanding of the data they need to work with.	You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.	

Monitoring staff do not have the correct specialist skills.	Monitoring staff can report to other parts of the organisation (e.g. security directors, resilience managers).	Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.	
Monitoring staff are not capable of reporting against governance requirements.	Monitoring staff are capable of following most of the required workflows.	Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external.	
Monitoring staff lack the skills to successfully perform some significant parts of the defined workflow.	Your monitoring tools can make use of logging that would capture most unsophisticated and untargeted attack types.	Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.	
Monitoring tools are only able to make use of a fraction of logging data being collected.	Your monitoring tools work with most logging data, with some configuration.	Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.	
Monitoring tools cannot be configured to make use of new logging streams, as they come online.	Monitoring staff are aware of some essential functions and can manage alerts relating to them.	Monitoring staff and tools drive and shape new log data collection and can make wide use of it.	
Monitoring staff have a lack of awareness of the essential functions the organisation provides, what assets relate to those functions and hence the importance of the logging data and security events.		Monitoring staff are aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them.	

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

A.6 APPENDIX E

Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	Comments
Normal system behaviour is insufficiently understood to be able to use system abnormalities to detect malicious activity.	Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (e.g. you fully understand which systems should and should not communicate and when).	
You have no established understanding of what abnormalities to look for that might signify malicious activities.	System abnormality descriptions from past attacks and threat intelligence, on yours and other networks, are used to signify malicious activity.	SOCOS
	The system abnormalities you search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential functions.	We prioritise (DLUHC?
	The system abnormality descriptions you use are updated to reflect changes in your networks and information systems and current threat intelligence.	No clearly defined feedback loop

Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	Comments

You do not routinely search for system abnormalities indicative of malicious activity.	You routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of your essential function, generating alerts based on the results of such searches.	3rd party Intergence contract plus in-house CISM expertise. However due to **resourcing/ recruitment** in-house expertise resource is sporadic
	You have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity.	3rd party Intergence contract plus in-house CISM expertise. However due to **resourcing/ recruitment** in-house expertise resource is sporadic

CAF Objective D - Minimising the impact of cyber security incidents
Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

Principle: D1 Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response Plan	**Not achieved - At least one of the following statements is true**	**Partially achieved - All of the following statements are true**	**Achieved - All the following statements are true**
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.	Your incident response plan is not documented.	Your response plan covers your essential functions.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	Your incident response plan does not include your organisation's identified essential function.	Your response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	Your incident response plan is not well understood by relevant staff.	Your response plan is understood by all staff who are involved with your organisation's response function.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function.
	DRAFT to be discussed/ recommended for adoption by Cyber T&F group.	Your response plan is documented and shared with all relevant stakeholders.	

D1.b Response and Recovery Capability	**Not achieved - At least one of the following statements is true**	**Achieved - All the following statements are true**

You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.	Inadequate arrangements have been made to make the right resources available to implement your response plan.	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.
	Your response team members are not equipped to make good response decisions and put them into effect.	You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available.
	Inadequate back-up mechanisms exist to allow the continued operation of your essential function during an incident.	Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out.
		Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function.
		Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable.

		Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).	

D1.c Testing and Exercising	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.	Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas.	Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence.	
	Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.	Exercise scenarios are documented, regularly reviewed, and validated.	
	Outputs from exercises are not fed into the organisation's lessons learned process.	Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned.	
	Exercises do not test all parts of the response cycle.	Exercises test all parts of your response cycle relating to your essential functions (e.g. restoration of normal function levels).	

Principle: D2 Lessons Learned	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	

D2.a Incident Root Cause Analysis	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	You are not usually able to resolve incidents to a root cause.	Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.	
	You do not have a formal process for investigating causes.	Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.	
		All relevant incident data is made available to the analysis team to perform root cause analysis.	

D2.b Using Incidents to Drive Improvements	Not achieved - At least one of the following statements is true	Achieved - All the following statements are true	
Your organisation uses lessons learned from incidents to improve your security measures.	Following incidents, lessons learned are not captured or are limited in scope.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon.	
	Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems.	

		You use lessons learned to improve security measures, including updating and retesting response plans when necessary.	
		Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.	
		Analysis is fed to senior management and incorporated into risk management and continuous improvement.	

Principles & Related Guidance
https://www.ncsc.gov.uk/collection/caf/table-view-principles-and-related-guidance