Senedd Cymru
Welsh Parliament

Telephony and networks

28 February 2022

Request for Information.

Thank you for your request received on 8 February 2022 in which you asked:

Contract 1 - Telephony/Voice Services (Analogue, ISDN VOIP, SIP etc)

1. *Telephony/Voice Services Provider- Please can you provide me with the name of the supplier for each contract.*
2. *Telephony/Voice Services - Contract Renewal Date- please provide day, month and year (month and year are also acceptable). If this is a rolling contract, please provide me with the rolling date of the contract. If there is more than one supplier, please split the renewal dates up into however many suppliers*
3. *Telephony/Voice Services - Contract Duration- the number of years the contract is for each provider, please also include any contract extensions.*
4. *Telephony/Voice Services - Type of Lines - Please can you split the type of lines per each supplier? PSTN, Analogue, SIP, ISDN, VOIP*
5. *Telephony/Voice Services Number of Lines / Channels / SIP Trunks- Please can you split the number of lines per each supplier? SIP trunks/connections, PSTN, Analogue, ISDN*

Contract 2 - Incoming and Outgoing of call services.

6. *Minutes/Landline Provider- Supplier's name (NOT Mobiles) if there is no information available, please can you provide further insight into why?*
7. *Minutes/Landline Contract Renewal Date- please provide day, month and year (month and year is also acceptable). If this is a rolling contract, please provide me with the rolling date of the contract.*

Senedd Cymru
Bae Caerdydd
Caerdydd, CF99 1SN

Welsh Parliament
Cardiff Bay
Cardiff, CF99 1SN
Ffôn/Tel: 0300 200 6224
E-bost/Email: Ceisiadau-gwybodaeth@senedd.cymru
Information-request@senedd.wales

8. *Minutes Landline Monthly Spend- Monthly average spend on calls for each provider. An estimate or average is acceptable. If SIP services, please provide me with the cost of services per month.*
9. *Minute's Landlines Contract Duration- the number of years the contract is for each provider, please also include any contract extensions.*
10. *Number of Extensions- Please state the number of telephone extensions the organisation currently has. An estimate or average is acceptable.*

Contract 3 - The organisation's broadband provider.

11. *Broadband Provider- Supplier's name if there is not information available, please can you provide further insight into why?*
12. *Broadband Renewal Date- please provide day, month, and year (month and year is also acceptable). If this is a rolling contract, please provide me with the rolling date of the contract. If there is more than one supplier, please split the renewal dates up into however many suppliers*
13. *Broadband Annual Average Spend- Annual average spend for each broadband provider. An estimate or average is acceptable.*

Contract 4 - Contracts relating to Wide Area Network [WAN] services, this could also include HSCN network services.

14. *WAN Provider- please provide me with the main supplier(s) if there is no information available, please can you provide further insight into why?*
15. *WAN Contract Renewal Date- please provide day, month, and year (month and year are also acceptable). If this is a rolling contract, please provide me with the rolling date of the contract. If there is more than one supplier, please split the renewal dates up into however many suppliers*
16. *Contract Description: Please can you provide me with a brief description for each contract*
17. *The number of sites: Please state the number of sites the WAN covers. Approx. will do.*
18. *WAN Annual Average Spend- Annual average spend for each WAN provider. An estimate or average is acceptable.*
19. *For each WAN contract can you please provide me with information on how this was procured, especially around those procurement that used frameworks, please provide me with the framework reference.*
20. *Internal Contact: please can you send me their full contact details including contact number and email and job title for all the contracts above.*

We confirm we hold the information requested and the information we are able to disclose is contained within the table below. However, a full disclosure will not be made as some of the information requested is exempt from disclosure under the Freedom of Information Act 2000 ("the Act"). The withheld information is indicated by the use of 'xxx'.

We consider that providing you with a full disclosure would indicate how we manage our internal secure systems which would make our systems vulnerable to malicious attacks.

We consider three exemptions apply which, in brief, are as follows:

1. section 24 – withholding the information is required for the purpose of safeguarding national security; and
2. section 31(1)(a) – disclosure of the information would, or would be likely, to prejudice the prevention of crime.
3. section 38(1)(a) & (b) – the information includes information that could endanger the physical or mental health of any individual, or endanger the safety of any individual.

Fuller details of the exemptions which have been applied, and the reasons for their application, are set out in the **annex** to this letter.

Contract 1

1. *xxx.*
2. *The contract has a renewal date of August 2023.*
3. *4 years*
4. *SIP*
5. *3 SIP trunks*

Contract 2

6. *xxx supply Voiceflex lines.*
7. *The contract has a renewal date of August 2023.*
8. *£600 per month*
9. *4 years*
10. *988*

Contract 3

11. xxx
12.

Supplier	***Start Date***	***Term***
Xxx	*07/21*	*12 months*

13.

Supplier	***Average Spend***

Xxx	*£41,000* approx

Contract 4

14. *xxx*
15.

Supplier	***Renewal date***
1x xxx Tŷ Hywel	*31/10/22*
1x xxx Tŷ Hywel	*31/10/22*
1x xxx Colwyn Bay	*31/10/22*

16.

Supplier	***Description***
1x xxx Tŷ Hywel	*Main Internet Link*
1x xxx Tŷ Hywel	*Backup Internet Link*
1x xxx Colwyn Bay	*Colwyn Bay Internet* Link

17.

Supplier	***WAN Sites***
Xxx	3

18.

Supplier	***Average Spend***
xxx	*£21,474 per year*

19. The framework used was a Welsh Government Framework.

20. Jan Koziel – Head of Procurement - **jan.koziel@senedd.wales**

Yours sincerely

Buddug Saer
Freedom of Information Manager
Welsh Parliament

Your request has been considered according to the principles set out in the **Code of Practice on Public Access to Information**. If you have any questions regarding this response please contact me. If you feel you have cause for complaint, please follow the guidance below.

Cause for concern or complaint with your FOI response?

If you are dissatisfied with the Welsh Parliament's handling of your request, you can request an internal review within 40 working days of the date of this response. Requests for an internal review should be addressed to the Freedom of Information Manager at:

Information-request@senedd.wales or in writing to

Welsh Parliament
Governance and Assurance
Cardiff Bay
Cardiff
CF99 1SN

Annex
Section 24

Section 24(1) of the Act provides:-

- *Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.*

We consider it necessary to withhold this information in order to maintain the integrity and robustness of the ICT infrastructure of the Senedd Commission ("Commission") and all the data, including personal data, that we hold. In turn, this enables us to ensure the safe and effective functioning of the Senedd as a legislature.

The information covered by this exemption relates directly to the software and operating systems in use by the Commission. Were the system to be compromised, our resources and data would be vulnerable to access, disclosure, alteration or destruction. The risk in the disclosure of this information is that there is a genuine likelihood it would damage the effectiveness and integrity of those systems and, in turn, the functioning of the Senedd.

The integrity and robustness of our ICT systems is paramount to the functioning of both the Commission and the Senedd and, as a parliament, we are categorised as a **Tier one site**. The operation of the CCTV system is an example of the need to maintain the integrity of our ICT system in order to ensure the security of the estate. Were the CCTV and access control systems to be impaired, there is a real possibility that it would leave the Senedd estate extremely vulnerable, as we would not be able to identify any hostile approaches or manage any unlawful activities. By maintaining effective controls we are able to ensure that Senedd Members, Senedd Member Support Staff, Senedd Commission staff, and visitors to the Senedd estate are not put at risk.

This exemption is a qualified exemption, and as such, the public interest in upholding the exemption must be considered. The public interest consideration for disclosure is that the public have a right to know and be satisfied that there are adequate ICT systems in place

in the Commission and the Senedd. There is also a clear public interest in ensuring transparency and accountability for public authorities.

It is our opinion, however, that the release of this information would materially damage the integrity and effectiveness of the Senedd's ICT security arrangements and security systems and therefore, in this instance, the public interest in withholding the information outweighs the public interest in its disclosure.

However, in order to ensure transparency and accountability to the extent that we are able, we have provided much of the other information you have requested, such as the length and costs associated with relevant contracts.

Section 31

Section 31(1) of the Act provides:-

- *Information which is not exempt information by virtue of section 30 is exempt information if the disclosure would, or would be likely to, prejudice –*
  (a) the prevention or detection of crime…

The operation of this exemption involves a number of steps:

- One of the law enforcement interests protected by section 31 must be harmed by the disclosure;
- The prejudice claimed must be real, actual or of substance;
- The public authority must be able to demonstrate a causal link between the disclosure and the harm claimed;
- The public authority must then decide what the likelihood of the harm actually occurring is (i.e. would it occur, or would it only be likely to occur).

The more certain the prejudice, the greater weight it carries when considering the public interest. In this context, the term "would prejudice" means that it has to be more probable than not that the prejudice would occur. "Would be likely to prejudice" is a lower level. Either way, there must be a real and significant risk.

Information can only be withheld under section 31 if its disclosure would, or would be likely to, prejudice one of the activities listed in either subsection (1) or (2). The relevant activity here is "the prevention or detection of crime" as listed in subsection (1)(a).

Section 31(1)(a) covers all aspects of the prevention and detection of crime. This exemption may be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime. So, the public authority may rely on the exemption in order to protect information on or about its systems, the disclosure of which would make it more vulnerable to crime. The information covered by this exemption relates directly to the software and operating systems in use by the Commission, including the disclosure of our ICT software systems, the supplier and/or vendor names of those systems, the operating systems and infrastructure services.
Our arguments against disclosure are:

- The Commission has a duty as a controller to ensure the security of the personal data that we hold. Making a disclosure would undermine our ability to meet that duty;
- The Commission has a duty to provide to the Senedd the services it requires to perform its functions. Similarly, a disclosure would undermine our ability to meet that duty; and
- A disclosure would leave our data vulnerable to access, disclosure, alteration or destruction. In turn this may lead to crimes including offences against property, offences against persons, public order offences, fraud, or digital vandalism.

The prejudice test is not limited to the harm caused by the requested information on its own. Account can be taken of any harm likely to arise if the requested information were put together with other information already known to the requester or in the public domain. It is also appropriate to consider the precedent that could be set for future requests by disclosing information about our security arrangements.

Our view, having considered the effect that disclosure could have on the integrity of the Senedd and its ICT infrastructure, is that to disclose the requested information would place at risk the security of the Commission's systems and, as a result of that, the security of the Senedd and those who work on and visit the Senedd estate. This would lead to prejudice to the prevention or detection of crime.

We then went on to consider the public interest test. As part of this test, there is a need to balance the security of the Senedd and its ICT infrastructure against the public interest in holding the Commission to account.

There is a clear public interest in protecting society from the impact of crime. There is also a clear public interest in the Commission being transparent in its processes and systems so that it can be held to account as a public authority.

The greater the potential for a disclosure to result in crime, the greater the public interest in maintaining the exemption. The victims of crime can be both organisations and individuals, but, in our view, there is a greater public interest in protecting individuals from the impact of crime. By disclosing information that could allow the identification of vulnerabilities in the Senedd ICT infrastructure, individuals who work on and visit the

Senedd estate would be placed at a greater risk of crime. In addition, individuals and organisations who engage with our outreach team, communications team and committee service could also be put at risk, if our systems were ever compromised.

In this case, it is our view that the public interest in favour of disclosure does not outweigh the need to protect the integrity of the ICT infrastructure in place to protect the Senedd, and those who work there.

However, in order to ensure transparency and accountability to the extent that we are able, we have provided much of the other information you have requested, such as the length and costs associated with relevant contracts.

Section 38

Section 38(1) of the Act provides:-

- *Information is exempt information if its disclosure under this Act would, or would be likely to —*
  (a) endanger the physical or mental health of any individual, or
  (b) endanger the safety of any individual.

The focus of section 38 is on information that might pose a risk if disclosed. This includes information that could lead to a risk to the physical or mental health of any individual, or the safety of any individual.

Section 38 is subject to an endangerment test. We must, therefore, be satisfied that there is a causal link between the endangerment and disclosure of the information.

The information requested details the specifics of our telecoms systems, our broadband provider and Wider Area Network (WAN). Disclosure of this information could assist an cyberattack on the Senedd's ICT infrastructure by allowing potential attackers to identify and exploit weaknesses that may exist in the Senedd's ICT infrastructure. Our systems contain payroll information, personnel files, information relating to Members of the Senedd and medical records held by the occupational health nurse, as well as other sensitive and personal information.

Such an attack could lead to the exposure of or risk to that information and could result in its unlawful use or release into the public domain. This would, or would be likely to, have the following effects:

- Endanger the mental health of any individual through the exposure of information, such as health or payroll information, that may have a distressing, physiological impact on those individuals and/or worsen a pre-existing mental illness;
- Endanger the physical health of any individual by exposing personal information, such as residential addresses; and
- Endanger the safety of any individual, including Members, support staff and Commission staff, through the exposure of personal information, such as residential addresses.

Some people or groups of society are particularly vulnerable, and their safety may be more easily endangered than others. This includes public facing figures, such as Members of the Senedd, who are required to publicly express their political views. This can bring them into conflict with individuals or groups who may hold opposing views and seek to cause them, and those around them, harm as a result.

It is notable that certain information related to Members of the Senedd, such as their residential address, information relating to certain travel arrangements, information relating to goods delivered to or services provided at their residential address, and information relating to expenditure on security arrangements, is specifically excluded from the scope of the Freedom of Information Act 2000.

Where information that could endanger an individual's safety could also endanger their mental or physical health, both parts of the exemption may be relied upon. In this situation, an endangerment to an individual's safety would be likely to endanger their mental and/or physical health. For example, an endangerment to safety could lead to an individual experiencing anxiety about their safety or those closest to them which results in mental harm, or even an endangerment to safety that leads to a physical attack.

This exemption is a qualified exemption and, as such, the public interest in upholding the exemption must be considered. This involves weighing up the risks to the health and safety of an individual or group against the public interest in disclosure in all circumstances of the case. This test must be applied on a case by case basis.

There is a clear public interest in promoting transparency and accountability by public authorities for decisions taken by them and in the spending of public money. There is also a public interest in allowing individuals, companies and other bodies to understand decisions made by public authorities. This includes the contracts they enter into and the suppliers they use.

However, there is also a strong public interest in withholding information that would undermine systems put in place to protect the health and safety of individuals or groups, as well as protect known individuals, such as public facing figures, from being targeted. This includes withholding information that could undermine cybersecurity.

Once section 38 is engaged and it has been established that there is a real and actual danger to someone's health and safety, it is difficult to find in favour of disclosure. We consider that to be the case in this instance. Our view is that the public interest in favour of disclosure does not outweigh the need to protect the integrity of the Senedd's ICT infrastructure and the information held within it, in order to protect the health and safety of individuals.

However, in order to ensure transparency and accountability to the extent that we are able, we have provided much of the other information you have requested, such as the length and costs associated with relevant contracts.