SOUTH WEST WALES CORPORATE JOINT COMMITTEE

7th October 2022

Report of the Monitoring Officer

Report Title: Adoption of Data Protection and Information Security Policies for the South West Wales Corporate Joint Committee

Purpose of Report	To adopt Data Protection and Information Security Polices
Recommendation	It is recommended that: (a) Members designate the Monitoring Officer as the Statutory Data Protection Officer pursuant to the Data Protection Act 2018; (b) Members adopt the Privacy Statement included at Appendix 1 (c) Members adopt the following policies for usage by the South West Wales Corporate Joint Committee included at Appendix 2: • Data Protection Policy • Acceptable Use Policy • Incident Reporting Policy • Information Security Policy • Information Security Breach Policy

	• IT Security Policy • Mobile Device Security Policy • Removable Media Policy
Report Author	Craig Griffiths
Finance Officer	N/A
Legal Officer	Craig Griffiths

Background:

The purpose of this report is to agree the designation of a Data Protection Officer for the CJC and also to adopt a suite of policies and protocols in respect of data protection and information governance.

Data Protection Officer.

The UK GDPR introduces a duty on public bodies such as the CJC to appoint a data protection officer (DPO) if it carries out certain types of processing activities such as the hold of personal information. DPOs assist orgnaisations to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO). The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. A DPO can be an existing employee or externally appointed. DPOs can help to demonstrate compliance and are part of the enhanced focus on accountability.

IT would be proposed to meet this requirement that the Monitoring Officer of the CJC also be designated the DPO of the CJC.

Policies

In order to meet legal requirements in respect of data procection and to provide the appropriate assurances to individuals whose data the CJC may be processing, it would be a requirement for the CJC to have a number of policies in place.

Appendix 1 includes a proposed privacy notice which will be held by the Monitoring Officer and available to the public in the event they are required to provide personal data to the CJC. This demonstrates the legal basis of

processing the data and includes information as to how the CJC will protect such data.

Appendix 2 includes a number of policies which the CJC will be required to adopt:

- Data Protection Policy – This is a policy required by the Data Protection Act 2018 which explains principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

- Acceptable Use Policy – This sets out the requirements that members/officers and other associated individuals with the CJC must take when accessing any computer equipment provided by the CJC (if any)

- Incident Reporting Policy – This is a policy that must be followed where individuals identify an incident may have occurred which could see the unauthorised release of personal data.

- Information Security Policy – This is a policy that sets out the various different forms of security that the CJC will have in place to prevent the unauthorised release of personal data.

- Information Security Breach Policy - This is a policy that must be followed where individuals identify an incident may have occurred which could see the unauthorised release of personal data and the steps that will be taken by the officers of the CJC to investigate and deal with.

- IT Security Policy - This is a policy required by the Data Protection Act 2018 which explains principles which we will apply to any IT process we undertake so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

- Mobile Device Security Policy – This is a policy which stipulates that steps must be taken to ensure any equipment provided the CJC is kept safe and secure.

- Removable Media Policy – This is a policy which prevents the use of removable media such as USB Sticks or Compact Discs being used without prior approval.

Financial Impacts:

There are no impacts associated with these policies.

Integrated Impact Assessment:

The CJC is subject to the Equality Act (Public Sector Equality Duty and the socio-economic duty), the Well-being of Future Generations (Wales) Act 2015 and the Welsh Language (Wales) Measure, and must in the exercise of their functions, have due regard to the need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Acts.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.
- Deliver better outcomes for those people who experience socio-economic disadvantage
- Consider opportunities for people to use the Welsh language
- Treat the Welsh language no less favourably than English.
- Ensure that the needs of the present are met without compromising the ability of future generations to meet their own needs.

The Well-being of Future Generations (Wales) Act 2015 mandates that public bodies in Wales must carry out sustainable development. Sustainable development means the process of improving the economic, social, environmental and cultural well-being of Wales by taking action, in accordance with the sustainable development principle, aimed at achieving the 'well-being goals'.

Workforce Impacts:

No impacts.

Legal Impacts:

All policies have been prepared in accordance with statutory requirements and will ensure the CJC can meet its legislative obligations

Risk Management Impacts:

Failure to ensure suitable data protection and information security policies in place can render the CJC open to legal challenge, with the financial and reputational issues that such action can bring. Ensuring that suitable policies are in place allows the CJC to discharge its legislative obligations.

Consultation:

There is no requirement for external consultation on these policies

Reasons for Proposed Decision:

To meet legal requirements in respect of data protection and information security.

Implementation of Decision:

To be implemented immediately

Appendices:

Appendix 1 – Privacy Statement
Appendix 2 – Suite of Data Protection/Information Security Policies

List of Background Papers:

None