Date signed off by the Monitoring Officer: N/A
Date signed off by the Section 151 Officer: N/A

Committee:	**Corporate Overview Scrutiny Committee**
Date of meeting:	**22 January 2021**
Report Subject:	**Information Security Policy**
Portfolio Holder:	**Cllr. Nigel Daniels, Leader of the Council & Executive Member Corporate Services**
Report Submitted by:	**Rhian Hayden, Chief Officer Resources**

Directorate Management Team	Corporate Leadership Team	Portfolio Holder / Chair	Audit Committee	Democratic Services Committee	Scrutiny Committee	Executive Committee	Council	Other (please state)
	7/1/21	11.01.21			22/01/21		28/01/21	Information Governance Forum – 18/12/20

1. Purpose of the Report

1.1 To provide Members with an opportunity to scrutinise the revised Information Security Policy and recommend its adoption by the Council.

2. Scope and Background

2.1 The attached document is the proposed Information Security Policy for the Council which sets out the approach the Council has adopted to develop, manage and improve Information Security to ensure our valuable information resources are properly protected.

2.2 The draft Policy has been revised and updates / replaces a number of the Council's current policies including:-

- Information Security Policy Statement
- Antivirus Policy
- Clear Desk Policy
- Disposal of IT Equipment Policy
- Information Assets Protection Policy
- Third Party Access Policy

2.3 The Policy applies to all Blaenau Gwent County Borough Council employees, Schools, volunteers, Members, contractors, third parties and all other authorised users with access to the Council's information assets.

2.3 The Policy identifies the general principles of Information Security i.e. confidentiality, integrity & availability, explains the roles and responsibilities of all parties with access to the Council's information and details the Council's expectations in ensuring that information remains secure.

2.4 The Policy emphasises that all security breaches must be reported immediately.

3. **Options for Recommendation**

3.1 **Option 1:** (preferred option) The Corporate Overview Scrutiny Committee considers the attached policy and recommends the Council approves the Policy.

Option 2: The Corporate Overview Scrutiny Committee comment and suggest amendments/additions to the Policy prior to recommendation to the Council.

3.2 The Policy was considered by the Information Governance Forum on 18 December 2020 and CLT on 7 January 2020, both supported the proposed policy.

4. **Evidence of how does this topic supports the achievement of the Corporate Plan / Statutory Responsibilities / Blaenau Gwent Well-being Plan**

4.1 **Statutory Responsibility:**
Information Security takes full account of a range of legislation, including the Data Protection Act and General Data Protection Regulation, governing the manner in which information and data is managed and protected.

5. **Implications Against Each Option**

5.1 *Impact on Budget*
There is no direct impact upon the budget as a result of implementing this policy, however, compliance with the policy will minimise data breaches and avoid financial penalties that could be imposed by the Information Commissioner.

5.2 *Risk*
Failure to comply with the Information Security Policy could result in loss or unintended disclosure of the Council's information assets resulting in significant reputational damage and imposition of financial penalties.

Development and implementation of and compliance with the Information Security Policy will mitigate this risk by ensuring all parties understand their responsibilities and the Council's expectations.

5.3 *Legal*
Information Security takes full account of a range of legislation, including the Data Protection Act and General Data Protection Regulation, governing the manner in which information and data is managed and protected.

5.4 *Human Resources*
The Policy applies to all Blaenau Gwent County Borough Council employees, Schools, volunteers, Members, contractors, third parties and all other authorised users with access to the Council's information assets.

Failure to comply with this policy may lead to disciplinary action.

6. Supporting Evidence

6.1 *Performance Information and Data*
n/a

6.2 *Expected outcome for the public*
Development, implementation and compliance with the Information Security Policy will provide assurance to the public that their personal, sensitive information held by the Council is secure and used appropriately.

6.3 *Involvement (consultation, engagement, participation)*
The Policy was developed in consultation with the Council's Information Governance Forum.

6.4 *Thinking for the Long term (forward planning)*
Compliance with the Policy will minimise the likelihood of data breaches. The Policy will be reviewed on an annual basis to ensure it remains appropriate.

6.5 *Preventative focus*
Compliance with the Policy will minimise the likelihood of data breaches.

6.6 *Collaboration / partnership working*
n/a

6.7 *Integration (across service areas)*
The Policy applies to information users in all service areas.

6.8 *EqIA (screening and identifying if full impact assessment is needed)*
The Policy has no impact on protective characteristics.

7. Monitoring Arrangements

7.1 Compliance with the policy will be monitored through the Council's performance management arrangements. Data Breaches will be reported to the Data Breach Group who will determine whether incidents should be reported to the Information Commissioners Office.

Background Documents /Electronic Links

Appendix 1 – Information Security Policy