Data Protection Policy

Cyngor Bwrdeisdref Sirol
Blaenau Gwent
County Borough Council

Security Classification: OFFICIAL
Handling Instructions: Internal Use Only

Document Reference:
Version: 2.3
RELEASE

Document Owner: Data Protection & Governance Officer

Document Author: Paul Amos

Authorisation & Document Control:

Document Owner:	Managing Director
Approved by:	Rhian Hayden (Chief Officer Resources/ SIRO)

Document History

Author	Version	Date	Review Date	Reason for Change
Paul Amos	2.0	23/04/ 2018	01/04/2019	Updated to reflect new legislation – GDPR and UK DPA 18
Paul Amos	2.1	31/05/ 2018		Incorporate suggested amendments made by the GDPR project team
Paul Amos	2.2	30/06/ 2018		Further amendments to layout and DPIA
Paul Amos	2.3	30/09/ 2018		IGF Comments

Document References

Ref	Document Reference	Title

Definitions

Title	Definition
GDPR	General Data Protection Regulation 2016
DPA	Data Protection Act 2018

Contents

1. Purpose

The policy provides information about the Data Protection principles and how BGCBC expects personal information to be handled. It outlines the roles and responsibilities of BGCBC Employees, Members and Partners in relation to Data Protection.

This policy has been developed to manage the way in which the authority complies with its Data Protection obligations and provide individuals with assurance that there are effective governance arrangements in place.

2. Policy statement

Everyone has rights with regard to how their personal information is handled. During the course of Blaenau Gwent County Borough Council (BGCBC) activities we will collect, store and process personal information, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers, and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and UK Data Protection Act (DPA). This legislation imposes restrictions on how we may use that information.

This policy will apply to all employees and members of BGCBC when processing personal data for and on behalf of BGCBC. This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

3. Status of the policy

This policy has been approved by full Council, and has the support of the Corporate Leadership Team. It sets out BGCBC rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

The Senior Information Risk Officer (SIRO) is responsible for ensuring compliance with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection & Governance Officer

If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager, if necessary your line manager will refer the matters raised to the Data Protection & Governance Officer.

4. Risk of non-compliance

The Council's main risks with regard to data fall into two key areas:

Information about individuals falling into the wrong hands, through poor security or inappropriate disclosure of information:

- Accidental loss of data
- Deliberate theft of data
- Lack of vigilance by staff or lack of training

Individuals being harmed through data being inaccurate or insufficient:

- Vulnerable people put at risk
- Inappropriate action taken by the Council, such as incorrect legal action

The Council seeks to minimise these risks through the use of appropriate physical and electronic data security, policies, procedures, training and guidance.

5. Definition of data protection terms

1. **General Data Protection Regulation (GDPR) 2016**, effective from 25th May 2018, is the EU law on data protection and privacy for all individuals within the Europe. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

2. **Data Protection Act 2018 (DPA)** is the main UK legislation which makes provision for GDPR into UK law. It also provides derogations for certain processing activities.

3. **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4. **Anonymised information** is information from which no individual can be identified.

5. **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

6. **Personal data** means data relating to a living individual who can be identified from that data and other information in our possession, or is likely to come into our possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

7. **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used within the Authority.

8. **Data users** include all employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

9. **Data processors** include any person who processes personal data on behalf of BGCBC. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

10. **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

11. **Special Category personal data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or data concerning a person's sex life or sexual orientation.

12. **Data sharing** relates to the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of data between different parts of an organisation. It can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

13. **Data sharing agreements/protocols** set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

14. **Privacy notice** is information provided to data subjects in relation to how their personal information is collected, handled and processed.

15. **Data Protection Impact Assessment (DPIA)** is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

4. Data protection principles

Employees of BGCBC and all its members that process personal data must comply with the enforceable principles of data protection that are set out under article 5 of the GDPR. These provide that personal data must be:

- Processed lawfully, fairly, and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There are also additional requirements set outside of the main principles, these include:

- Accountability; the Council shall be responsible for, and be able to demonstrate compliance with all of the principles listed above.
- International transfers; personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data
- Individual's Rights; covered under section 11 below.
- Data Protection Impact Assessments; covered in Appendix 1 of this policy.

5. Fair and lawful processing

The Regulation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. **The data subject must be provided with a privacy notice** that confirms who the data controller is, in this case BGCBC, the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred. The Council's Privacy Notice is available on the corporate website.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, the performance of a public task, or that the processing is necessary for compliance with a legal obligation to which the controller is subject. When special category personal data is being processed, an additional condition must be met under article 9 of GDPR.

6. Processing for specified, explicit and legitimate purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by Data Protection legislation. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

7. Adequate, relevant and limited to what is necessary

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. Kept for no longer than is necessary

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, please see the Councils Corporate Records Retention and Disposal Policy.

10. Data security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Legal Department is responsible for advising on compliance with the GDPR. The Data Protection & Governance Officer is responsible for ensuring that BGCBC's information governance arrangements are fit for purpose, and for developing specific guidance notes and/or training on data protection for employees and Members of BGCBC.

Any infringement of the Data Protection Regulation by employees or Members may expose BGCBC and/or the individual to legal action, claims for substantial damages and fines from the Information Commissioner. Any infringement of the Regulation will be treated seriously by BGCBC and may be considered under disciplinary procedures.

All alleged breaches of the data protection policy shall be notified to the Data Protection and Governance Officer immediately. Where there has been an unauthorised disclosure of personal data the Data Protection and Governance Officer shall advise on any remedial action.

All serious alleged breaches of Data Protection will be referred to the Data Protection breach management group that includes the Senior Information Risk Officer (SIRO) and Head of Legal & Corporate Compliance, where it shall be considered whether the matter should be reported to the Information Commissioner.

The Regulation requires BGCBC to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes.

The Council's Information security policies and procedures are available to all employees and Members of BGCBC and can be found on the Intranet.

11. Individual's Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The legal basis being relied upon to use someone's personal information will affect the rights that the individual has in relation to their information. For example if relying upon the consent of the person to use their personal data, then the right to have their personal information erased is stronger. As such it is important to identify the correct legal basis from the outset.

Lawful Basis article 6	Right to Access	Right to Rectification	Right to Erasure	Right to Restrict processing	Right to Portability	Right to Object	Auto-decision making
Consent	Yes	Yes	Yes	Yes	Yes	No - but right to withdraw consent	No - but right to withdraw consent
Contract	Yes	Yes	Yes	Yes	Yes	No	No
Legal obligation	Yes	Yes	No	No	No	No	No
Vital interest	Yes	Yes	Yes	No	No	No	Yes
Public Task	Yes	Yes	No	No	No	Yes	Yes
Legitimate Interest	Yes	Yes	Yes	Yes	No	Yes	Yes

All requests should be referred to the Data Protection & Governance Officer. The Council will then inform the Individual whether the request has been granted and if it has been refused, the reasons for the refusal.

All requests should be responded to within 1 month.

12. Employees and Members Obligations

Employees and Members shall only process personal data that is under the control of, or on behalf of, BGCBC when there are lawful grounds to do so and where that employee and Member is so authorised by BGCBC to process that personal data.

Unauthorised processing of personal data by employees and Members includes accessing personal data records for private interest and/or gain, even where access to the record system itself has been granted to the same member for business purposes. Unauthorised processing of personal data also includes disclosure of personal data (including verbal disclosures) to a third party where it is known that the third party is not entitled to receive that data.

Unauthorised processing of personal data is a potential disciplinary matter which will be considered under the relevant disciplinary procedures. Serious breaches of the Regulation may constitute a criminal offence.

Employees and Members shall exercise personal responsibility in the secure handling of personal data and shall not knowingly or recklessly expose personal data to unauthorised access, disclosure or loss. Where employees and Members are unsure as to appropriate security measures they shall seek advice from their line manager and/or the Data Protection and Governance Officer.

Members of BGCBC are data controllers in their own right and are responsible for all personal data that they process.

Where employees and Members are unsure as to any of the provisions of the Regulation or this policy they shall seek advice from their line manager and/or the Legal Department.

13. Dealing with subject access requests

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Any member of staff who receives a request should forward it to the Information Governance team within the Legal Department immediately.

All subject access requests must be conducted in accordance with the organisational procedure.

A search for information following a subject access request should not be commenced until the identity of the requestor has been verified. Documents which provide acceptable verification are listed on the Subject Access Request form.

Information will normally be provided in permanent form, i.e. by hard or electronic copy, according to how the information is held and the wishes of the requestor. A requestor may also be granted supervised access to certain documents if this can be done without revealing any other person's personal information.

Care must always be taken to ensure that the personal data of any third party is not disclosed. When redaction of third party personal data destroys the sense of a document, a summary may be provided in its place.

BGCBC shall take steps as appropriate to ensure that data subjects are aware of both their rights and obligations and BGCBC's rights and obligations under the Regulation, and to make all employees, members, contractors and third parties aware of the Regulation and the implications of processing personal data.

14. Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Council. In particular they should:

Check the caller's identity to make sure that information is only given to a person who is entitled to it.

Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

Refer the matter to their line manager or contact the Data Protection and Governance Officer for assistance in difficult situations. No-one should be bullied into disclosing personal information.

15. Data Protection Officer

As a public authority we have appointed a Data Protection Officer (DPO). The DPO reports directly to the Senior Information Risk Officer (SIRO) and Information Governance Forum (IGF) and is given the required independence and sufficient resources to perform their role.

The DPO also covers all Schools within the borough of Blaenau Gwent.

The Council and Schools will involve the DPO, in a timely manner, in all issues relating to the protection of personal data.

The DPO shall not be penalised for performing their duties and the Council will ensure that any other tasks or duties assigned to the DPO do not result in a conflict of interests with their role as DPO.

Tasks of the DPO:

- monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits;
- provide advice and monitor the Data Protection Impact Assessment (DPIA) process;
- register (notify) under Data Protection Law with the ICO;
- act as a contact point for the ICO;
- has due regard to the risk associated with processing operations, and take into account the nature, scope, context and purposes of processing.

The Council and Schools will take account of our DPO's advice and the information they provide on data protection obligations.

The DPO can be contacted through: DataProtection@blaenau-gwent.gov.uk

16. Management Responsibility

Each department/service area has responsibility for the proper handling of all personal data and is responsible for drawing up local operational procedures which are consistent with this policy and corporate practice to ensure that good Data Protection practice is established and followed. This includes the use of information sharing protocols where there is a regular need to share personal data.

Managers must ensure that the Data Protection Officer is informed of any changes in their Service area's uses of personal data.

Data Protection Impact Assessments will be undertaken at an early stage whenever use of personal information is proposed and particularly during new collaborations.

A Record of Processing Activities (ROPA) is maintained by each Service Area, and the way that the information is processed will regularly be evaluated using Data Protection Impact Assessments where necessary.

Privacy notices will be created for all processing activities and communicated to Data Subjects in accordance with GDPR requirements.

Managers should also liaise with the Data Protection Officer in any situation where doubt exists over proper practice.

Managers are also responsible for ensuring that their staff are aware of the mandatory GDPR training. Individual officers are responsible for undertaking mandatory training as instructed.

Should any breaches of the GDPR and related data protection law be identified, such as accidental or malicious loss of data, the individual's line manager must report the loss to the Data Protection Officer as soon as possible, without delay.

The overall responsibility shall lie with the Head of Service, as outlined in the Information Asset Owner structure.

17. Information Asset Registers

The Council maintains an Information Asset Register (IAR) which identifies all core datasets and systems across the Council. This is supported by a Record of Processing Activities (ROPA) to provide more detailed information on specific processes, as required under GDPR.

The following information is documented within the IAR and ROPA:

- the categories of personal data being processed,
- the purpose of processing,
- the legal basis for processing,
- retention period,
- explicit consent (if applicable),

18. Monitoring and review of the policy

This policy will be monitored by the Data Protection and Governance Officer. The policy is based on legislation and will be kept under review in accordance with legislative requirements and with particular reference to changes in legislation.

Feedback relating to this policy can be made by telephone or via email to the Data Protection and Governance Officer, 01495 355080 or DataProtection@blaenau-gwent.gov.uk .

We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

Appendix 1: DPIA (Data Protection Impact Assessment)

This Assessment provides a set of responses aimed to reduce the impact of Data Protection risks identified within a project / processing activity.

When carrying out the Data Protection Impact Assessment we should consider any perceived risks to the data subjects, and also how the proposal may affect our compliance with the Principles of the GDPR (General Data Protection Regulation).

When is this necessary?

A Data Protection Impact Assessment is **mandatory** for any processing that falls under the following criteria;

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.
    - systematic and extensive processing activities, including profiling
    - and where decisions that have legal effects – or similarly significant effects – on individuals.
    - large scale processing of special categories of data or personal data relating to criminal convictions or offences.
- This includes:
    - processing a considerable amount of personal data at regional, national or supranational level;
    - that affects a large number of individuals; and
    - involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
    - large scale, systematic monitoring of public areas (CCTV).

Section One: Project background

[Note: To be completed by the relevant Service Manager or those designated with responsibility for the service]

Scope Provide background information regarding the processing, including its purpose, aims and objectives, scope, business rationale, benefits to the service user and / or organisation, constraints and relationships.
Describe the information flows Describe the collection, use and deletion of personal information and if the information flow process is a new or amended one e.g. paper process replaced by an electronic one or a new database which consolidates information held by separate parts of the organisation or multiple organisations. Include any potential new uses of personal information. It will be useful to provide a flow diagram or another way of explaining the information flows.

Special Category Personal Data

Confirm whether any of the Data falls within the special categories;
Convictions, Racial or ethnic origin; Political Opinions; Religious or philosophical beliefs; Trade Union; Genetic or Biometric data; Health; Sex life or Sexual orientation.

Supporting Information

Any additional supporting information, such as;

- Attachments – relevant documents to ensure this assessment is a complete record of what will be approved
- Approvals – evidence approvals obtained for the proposal

Section Two: Data Protection Impact Assessment

[Note: To be completed by the relevant Service Manager or those designated with responsibility for the service]

Privacy issue	Risk to individuals	Compliance Risk	Risk Score - Impact - Likelihood **Risk matrix attached to PIA**	Solution(s)	Residual Risk Score - Impact - Likelihood	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Processed lawfully, fairly and in a transparent manner	Unlawful invasion of privacy	Articles 5-9: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions under Article 6 of GDPR is met, and (b) in the case of **special category** personal data, at least one of the conditions in Article 9 of GDPR and a condition under Schedule 1 of the UK	Impact: Likelihood: **Score:**	Document the lawful basis for processing under the GDPR and Data Protection Act (if necessary). This information should be recorded within the Record of Processing Activities for your department. You must also ensure a privacy notice has been completed to	Impact: Likelihood: **Score:**	

		Data Protection Act 2018 is also met. Articles 12-14: The right to be Informed		comply with GDPR statutory requirements!		
Personal Data must be collected for specified, explicit and legitimate purposes	Potential safeguarding concerns Invasion of Privacy	Article 5, 1(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	
Adequate, Relevant and Limited	Excessive amount of Information stored concerning them	Article 5, 1(c): Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	

Accurate and, where necessary, kept up to date.	Detrimental effects on Data Subjects	Article 5, 1(d): Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	
Kept for no longer than is necessary	Misrepresentation of character	Article 5, 1(e): Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	

		personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.				
Appropriate Security	Detrimental effects on Data Subjects Safeguarding concerns	Article 5, 1(f): Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	

Transfers of personal data to third countries or international organisations	Detrimental effects on Data Subjects	Articles 44- 50: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	Impact: Likelihood: **Score:**	Is the country (or territory/ processing sector) or organisation approved by the EU/ICO as having an adequate level of protection? Are there appropriate safeguards in place in a legal contract/ agreement?	Impact: Likelihood: **Score:**	
Processed in accordance with the data subject's rights	Detrimental effects on Data Subjects	Articles 12- 23: Personal data shall be processed in accordance with the rights of data subjects.	Impact: Likelihood: **Score:**		Impact: Likelihood: **Score:**	

Solutions Approved by:

Relevant Service Manager:

Sign …… Print…… Date ……

Data Protection & Governance Officer:

Sign …… Print…… Date ……

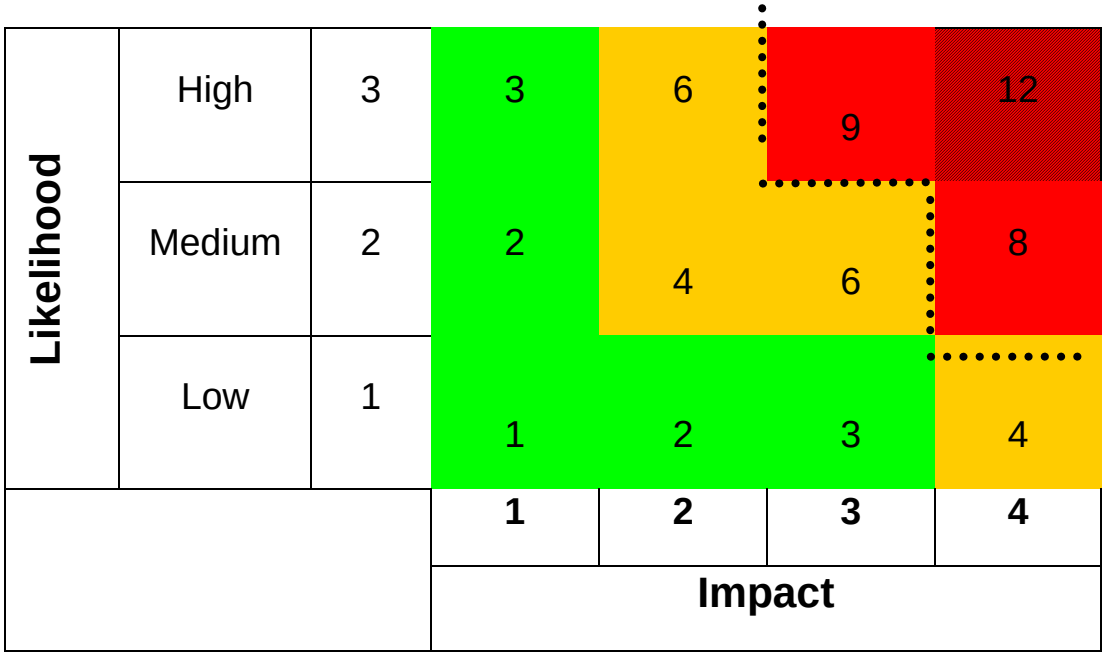
Where risks cannot be managed within the organisation's risk tolerance, the proposal can be escalated to the SIRO for consideration.

If a high risk is identified that it is not possible to mitigate, the Council must consult the ICO (Information Commissioner's Office) before they commence processing.

Impact	Sensitivity / Volume
1	Non-sensitive personal data available for public disclosure. Volume not applicable
2	Non-sensitive personal data that is not available for public disclosure, or <= 100 records
3	Sensitive Personal Data (E.g. trade union membership, physical or mental health or condition, the commission or alleged commission by him of any offence, financial records), or >= 100 records
4	Extremely sensitive personal data (e.g. more explicit details of individuals' circumstances, such as sexual abuse claims), or > 1000 records

Risk Definitions		
Project likelihood (the potential for the risk to occur is;)		
1	Low (unlikely)	Unlikely to occur, only in exceptional circumstances. (i.e. between 1%-25% probability)
2	Medium (possible)	Unlikely to occur, but could occur at some time. (i.e. between 25%-50% probability)
3	High (likely)	Almost certain to occur. (i.e. More than 50% probability)

Risk Matrix - Blaenau Gwent Council's risk tolerance.



Key	Low	Medium	High	Critical
	1 - 3	4 - 6	7 - 9	Above 10