HIGH PEAK BOROUGH COUNCIL

Report to the Corporate Select Committee

20 March 2017

TITLE:	**Revised Data Protection Policy**
PORTFOLIO:	**Councillor Thrane - Executive Councillor for Finance and Corporate Services**
OFFICER:	**Executive Director (People) and Monitoring Officer**
WARDS:	**All**

Appendices Attached: Appendix A - Draft Data Protection Policy

1. Reason for the Report

The Borough Council has a duty to process information fairly and lawfully and to comply with the data protection principles contained within the Data Protection Act 1998. A data protection policy assists the Council to meet its statutory requirements and is one of the key pieces of evidence looked for during any data protection audits carried out by the Information Commissioner's Office (ICO).

2. Recommendation

2.1 It is recommended that the Committee requests the Executive to approve the revised data protection policy.

3. Executive Summary

3.1 The Data Protection Act (DPA) 1998 stipulates that anyone processing personal data must comply with eight data protection principles. Failure to process personal data lawfully, accurately and fairly can lead to poor decision making, inefficient business processes, inconvenience or harm to residents and others, reputational damage to the Authority, or enforcement action by the Information Commissioner's Office.

3.2 A revised Data Protection policy is presented with the overarching aim of ensuring that the Council meets its requirements under the DPA. It also seeks to provide practical advice for staff members to ensure that we are processing data fairly and lawfully. The data protection policy sets out:

- practical steps to be followed to comply with the data protection principles;
- the responsibility of staff members when processing personal data;
- the Council's response to data breaches;
- how we will communicate privacy information to individuals;
- the Council's approach to data sharing;
- how we will use Privacy Impact Assessment;
- our approach to responding to requests for information; and
- information security procedures.

3.3 The policy applies to councillors when carrying out their role as a member of the Council. In such circumstances, councillors are carrying out the local authority's functions and so do not need to register with the Information Commissioner in their own right. Sections 3.5 to 3.12 of the revised policy provide specific guidance for councillors.

4. How this report links to Corporate Priorities

4.1 This is a cross-cutting policy that impacts on all Council priorities and services.

5. Options and Analysis

5.1 None. The Council needs an up-to-date data protection policy to mitigate the risk of misusing information.

6. Implications

6.1 Community Safety - (Crime and Disorder Act 1998)

The data protection policy would apply to the processing of community safety-related information.

6.2 Workforce

All staff members will be expected to operate under the policy in a manner that is compatible with the requirements of the Data Protection Act 1998.

6.3 Equality and Diversity/Equality Impact Assessment

Not applicable.

6.4 Financial Considerations

There will be some requirements for training officers and Elected Members but these costs will be met from existing budgets.

6.5 Legal

The policy seeks to ensure that the Council is compliant with the Data Protection Act 1998.

6.6 Sustainability

No specific implications.

6.7 Internal and External Consultation

N/A

6.8 Risk Assessment

Non-compliance with data protection principles can lead to poor decision making, inefficient business processes, inconvenience or harm to residents and others, reputational damage to the Authority, or enforcement action by the Information Commissioner's Office.

7. Background and Detail

7.1 High Peak Borough Council has to collect and use information about people to efficiently and effectively provide quality services for the local area. The Council may also be required by law to collect and use information to comply with the requirements of central government. The information collected by the Authority may include information about members of the public and businesses; customers and suppliers; and current, past and prospective employees and councillors.

7.2 The Data Protection Act (DPA) 1998 stipulates that anyone processing personal data must comply with eight data protection principles. These principles are legally enforceable and require that:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area[1] 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.

7.3 It is important that this collection and use of personal data is carried out lawfully, accurately and fairly. Failure to do so can lead to a range of problems including poor decision making, inefficient business processes, inconvenience or harm to residents and others, reputational damage to the Authority, or enforcement action by the Information Commissioner's Office.

7.4 The main powers available to the ICO are:

- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations' processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010;
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.

7.5 A revised data protection policy is provided at Appendix A. The overarching aim of the policy is to ensure that the Council meets the requirements of the DPA. It also seeks to provide practical advice for

[1] The European Economic Area[1] includes the EU member states plus Iceland, Liechtenstein and Norway.

staff members to ensure that we are processing data fairly and lawfully. The data protection policy sets out:

- practical steps to be followed to comply with the data protection principles;
- the responsibility of staff members when processing personal data;
- the Council's response to data breaches;
- how we will communicate privacy information to individuals;
- the Council's approach to data sharing;
- how we will use Privacy Impact Assessment;
- our approach to responding to requests for information; and
- information security procedures.

7.6 The policy applies to councillors when carrying out their role as a member of the Council. In such circumstances, councillors are carrying out the local authority's functions and so do not need to register with the Information Commissioner in their own right. Sections 3.5 to 3.12 of the revised policy provide specific guidance for councillors.

7.7 When acting on behalf of a political party then an Elected Member will normally be able to rely on the parties' registration (but independents will need to have their own registration). When councillors represent residents of their ward, they are likely to have to register in their own right. For example, if they use personal information to timetable surgery appointments or take forward complaints made by local residents.

7.8 The data protection policy forms an important part of the Council's overarching Information Governance strategy and should be read in conjunction with that strategy.

7.9 It should be noted that the General Data Protection Regulation (GDPR), which would supersede the Data Protection Act 1998, was on track to come into force in the UK on 25 May 2018. The result of the June 2016 referendum cast doubt on the introduction of the GDPR; however, the Secretary of State for Culture, Media and Sport has indicated that the country will ***"****opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."*

Mark Trillo
Executive Director (People) and Chief Monitoring Officer

Background Papers	**Location**	**Contact details**
		David Smith x 4165