ITEM NO. 8.1

Report of:	**Head of Governance & Corporate Services**
Contact Officer:	**Darren Edwards**
Telephone No:	**4447**
Portfolio Leader:	**Corporate Improvement**
Key Decision:	**No**
Report Track:	**Cabinet: 19/04/18**

CABINET
19 APRIL 2018
DATA PROTECTION POLICY

1 Purpose of Report

1.1 To seek Members' approval for the formal adoption of the Data Protection Policy.

2 Recommendations

2.1 That Cabinet approves and formally adopts the Data Protection Policy.

2.2 That the Head of Governance & Corporate Services, as the Senior Information Risk Owner, be given delegated authority to make amendments to the Data Protection Policy to reflect any changes in legislation.

3 Key Issues and Reasons for Recommendation

3.1 With the implementation of the General Data Protection Regulations (GDPR) on 25th May 2018, it is necessary to update the Council's current Data Protection Policy to ensure compliance.

3.2 The policy lays out how the Council will collect, store, handle and use any personal information it needs to carry out its work.

3.3 The policy applies to all employees, Elected Members, contractors, partners and any others working with personal information controlled by the Council. It is essential that the policy is complied with to ensure that the public have confidence in the Council and its handling of personal information. Failure to follow the policy and ensure that the Council abides by Data Protection legislation can result in the imposition of penalties upon the Council.

4 Relationship to Corporate Priorities

4.1 The processing of data is integral to the delivery of Council services and as such supports all of Corporate Priorities.

5 Report Detail

5.1 The policy describes how Cannock Chase Council will collect, store, handle and use any personal information it needs to carry out its work. It applies to all personal information held by the Council, such as personnel records, personal benefits information and housing tenants information.

5.2 The policy applies to all employees, Elected Members, contractors, partners and any others working with personal information controlled by the council. Details of roles and responsibilities are laid out in the policy.

5.3 So that we can deliver the services and standards our customers expect, Cannock Chase Council needs to collect and use personal information. Data Protection Legislation requires us to follow certain rules and have adequate processes in place to protect confidentiality in the processing of personal data.

5.4 The Data Protection Officer (DPO) has a key role in ensuring compliance with the policy and in accordance with GDPR they will have the right to report directly to the Managing Director and Members on any concerns. The DPO is also responsible for reporting data security breaches to the Information Commissioner.

5.5 The key changes that GDPR will bring in relation to the Council are:

- Data protection processes must be embedded in departmental operations.
- Additional requirements on fair processing notices to data subjects.
- Data assets and flows must be documented and mapped.
- Privacy impact assessments to be carried out where new systems containing personal data are to be implemented..
- Data subjects have the ‘right to be forgotten’ / right to erasure particularly where processing is based on the subject’s consent. (This would not apply to the processing of current cases for statutory purposes).
- Responsibility now falls on data processors as well as data controllers for security and processing of personal data.
- A Data Protection Officer must be appointed.
- Fines for non compliance increase from £500,000 to €20,000,000.
- Data breaches must be reported within 72 hours to the ICO.

- Subject access requests can no longer be charged for and the time to process such requests drops from 40 calendar days to 1 month.

6 Implications

6.1 Financial

The fee for registration (currently laid before Parliament) is due to increase from £500 to £2,500.

Fees for Subject access requests can no longer be charged. The fees were £5 per request (£10 for a repeated request) the removal of these fees may also spark an influx of such requests impacting on workload.

6.2 Legal

Referred to throughout the report.

6.3 Human Resources

None.

6.4 Section 17 (Crime Prevention)

Sharing information between agencies in Staffordshire is a statutory duty. This policy will help to ensure that data is being handled and shared correctly and legitimately by providing guidance to uphold the security of personal data.

6.5 Human Rights Act

None.

6.6 Data Protection

As set out in the report and in the policy itself.

6.7 Risk Management

The Data Protection policy provides a framework to support the secure processing of personal data; compliance will help to minimise the risk of security breaches which could damage the Council's reputation.

6.8 Equality & Diversity

An equality impact assessment has been completed.

6.9 Best Value

None.

ITEM NO. 8.4

7 Appendices to the Report

Appendix 1 Data Protection Policy

Previous Consideration

None.

Background Papers

None.

ITEM NO. 8.5

Appendix 1

Cannock Chase District Council

Data Protection Policy

Version 1.0
23 March 2018

Contents

1. Introduction

1.1 **Cannock Chase District Council** (the Council) takes its responsibilities with regard to the management of the requirements of Data Protection Legislation seriously.

2. Policy Statement

2.1 The Council is committed to compliance with the Data Protection Legislation.

2.2 The Council needs to process certain types of personal data (personal information) about the people with whom it deals in order to perform effectively as a Council. These people include current, past and prospective employees, service users, customers and clients and others with whom the Council communicates. This data must be dealt with properly when it is collected, recorded, used and destroyed whether by manual or electronic means. Extra care must be taken with sensitive personal data.

2.3 The Council regards the lawful and correct treatment of personal information as important to the successful operation of the Council's functions. Numerous records and systems containing personal information exist within the organisation and the integrity and quality of this information is paramount. The communities serviced by the Council expect data to be treated in line with legislation. If any breaches of Data Protection Legislation do take place then these will be dealt with in accordance with the policy.

3. Scope

3.1 This policy applies to all employees and workers (both contracted and agency workers), contractual third parties, agents and representatives, volunteers, and councillors (when acting on behalf of the Council).

3.2 This policy does not cover Councillors in regard to their constituency responsibilities, as they are data controllers in their own right and therefore are responsible for their own information compliance.

3.3 This policy applies to all personal data processed or controlled by the Council, in whatever format or however it is stored. This includes (but is not limited to) IT systems / databases, shared drive filing structures, email, paper records, videos and CCTV recordings.

4. Data Protection Principles

4.1 All Council staff processing personal data must comply with the Data Protection Principles which make sure that personal information is:

- Fairly, lawfully and transparently processed
- Collected and processed for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary
- Accurate and up to date
- Not kept for longer than is necessary
- Secure and protected against loss, theft and damage.

In addition the Council and it's staff must be able to demonstrate compliance with the principles.

5. Roles and Responsibilities

5.1 **The Council** is a data controller under the Data Protection Legislation.

5.2 **Members** - all elected members are to be made fully aware of this policy and of their duties and responsibilities under the Data Protection Legislation. When Members handle personal information in their role as elected members, they are covered by the Council's notification. As such, they have to handle personal information in line with the requirements of the data protection principles. If Members use (process) personal information in their constituency work, this activity is not generally covered by the Council's notification and they may have to notify with the Information Commissioner's Office as a separate data controller.

5.3 **Leadership Team** - has overall responsibility for ensuring that the Council and its staff complies with the Council's legal obligations regarding the handling of personal information and is responsible for ensuring compliance with this policy. In discharging this duty, Leadership Team will approve the corporate framework for data protection within the Council as set out in this policy to protect personal information.

5.4 **Senior Information Risk Owner (SIRO)** –is the member of the Leadership Team accountable for information risk management. They will ensure that information risks are identified and accounted for within the Councils systems of internal control. The Council's SIRO is the Head of Governance and Corporate Services.

5.5 **Service Managers** – shall promote good practice and assist the members of the Leadership Team to ensure compliance with Data Protection Legislation and with this policy. They act as a referral point for the services they represent in order to raise issues that may need to be addressed by Leadership Team.

5.6 **Data Protection Officer** (DPO) – is responsible for developing and keeping this policy up to date. They act as the lead advisor to the Council regarding compliance with the Data Protection Legislation and this policy. They will ensure that compliance is monitored across the Council and will act as the appropriate point of contact between the Council and the Information Commissioner. The Council's Data Protection Officer is the Information Manager.

5.7 **Information Manager** – responsible for the provision of day to day advice and assistance to Council employees on data protection issues, including assistance in responding to requests by individuals seeking to exercise their rights under the data protection legislation.

5.8 **Information Asset Owners (IAOs)** – have responsibility for any Council systems that hold or process personal data. Their role is to identify and control access to those systems and ensure that arrangements are in place to ensure information contained within those systems are processed in accordance with the Data Protection Legislation and this policy. Service Managers should ensure that IAO's are identified for each system within their service and that adequate training on data protection is provided to them. The service manager may elect to be the IAO or they may delegate this to an operational manager, team leader or supervisor who manages a system on a daily basis.

5.9 **All members of staff, contractors and elected Members** who hold or collect personal data are responsible for their own compliance with the Data Protection Legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with the Data Protection Legislation, and with this policy. In particular, staff must not attempt to access personal data that they are not authorised to view. Employees who fail to comply with the Data Protection Legislation may face disciplinary action which could lead to dismissal and, in some cases, criminal proceedings or prosecution.

6. Consequences of Non Compliance

6.1 An individual has the right to claim compensation for damage or distress suffered as a result of non-compliance, be it inappropriate processing or poor data quality. If an individual complains to the Information Commissioner's Office (ICO) then the Information Commissioner is obliged to investigate in order to establish if a breach of Data Protection Legislation occurred.

6.2 The Commissioner can serve a Data Controller with an 'Information Notice' requiring the Data Controller to provide certain information within set time limits. The deliberate provision of false information in response to an Information Notice is a criminal offence.

6.3 If the Commissioner decides that there had been a breach of the Data Protection Legislation, he may serve the Data Controller with an 'Enforcement Notice'. This may require the Council to carry out certain steps, or refrain from taking certain steps, specified in the notice.

6.4 The Commissioner can also prosecute those who commit criminal offences under the Data Protection Legislation, and conduct audits to assess whether an organisations processing of personal data follows good practice.

6.5 The Commissioner is able impose financial penalties on organisations as a penalty for breaches of the Data Protection Legislation, including for failure to comply with Information or Enforcement Notices.

7. Criminal Offences

7.1 There are a number of criminal offences under the Act. These include:

- Obtaining or disclosing personal data or the information contained in personal data without the consent of the Data Controller (Cannock Chase Council);
- Procuring the disclosure to another person of the information contained in personal data without the consent of the Data Controller.

7.2 After obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained. A full list of offences can be found on the Crown Prosecution Service (CPS) website.

7.3 In addition, in relation to computer processed information, the following are offences under the Computer Misuse Act 1990:

- Unauthorised access to computer;
- Unauthorised modification to contents of computer; and
- Unauthorised access with intent to commit/facilitate the commission of further offences.

8. Personal Interests and Connections

8.1 In situations where a member of staff has a personal connection with the data subject (for eg service user, customer, client) they must declare this connection, and the reason for the enquiry, to their manager before any action is taken. The manager will then consider any potential conflict of interest and allocate the enquiry to an independent person if deemed necessary.

8.2 This applies to relatives, in-laws, spouse or partner, neighbours, friends and former or present colleagues, or any other person whose personal connection to you could be perceived as likely affecting your ability to act impartially and professionally.

9. Breaches

9.1 Staff should only access systems and records containing personal information that are relevant to their work/duties.

9.2 In the event of a breach or a potential breach of data protection, either from an internal or external source, the Data Protection Officer must be notified as soon as possible, and in any case within 24 hours. Where a member of staff reports another, protection and anonymity will be afforded to those who request it in accordance with the Council's Confidential Reporting Policy.

9.3 Compliance with Data Protection procedures is taken very seriously and disciplinary action may be taken against any employee who breaches any instruction contained in, or arising from this policy.

9.4 Any breaches of security involving personal data must be dealt with in accordance with the procedures laid down in the Council's Data Protection Breach Protocol.

10. Subject Access Requests (SARs)

10.1 The Data Protection Legislation gives individuals the right to access personal information held about themselves by the Council and to be supplied with a copy of that information (subject to provisions).

10.2 SARs are co-ordinated by the Information Manager.

10.3 There is a one month time limit specified by the Act in which to comply with such requests.

10.4 Individuals requesting access to their records must provide details on the information they require and proof of identity. Individuals can access a subject access form on the Council's website to assist this process.

10.5 If a request is made through a third party acting on the data subject's behalf, that person will need to provide evidence of their identity and proof that they are entitled to act on the data subject's behalf. If they are a parent, foster parent or carer, acting on behalf of a child under 13 years of age, they will need to provide proof of parental responsibility (children 13 years of age or over would be expected to submit their own request).

10.6 The form should be returned to the Information Manager who will allocate the request to the appropriate team or department and provide advice and guidance in dealing with the request.

11. Rectification and Erasure

11.1 The Data Protection Legislation also gives individuals the right to have inaccurate personal data concerning them rectified, to request that any personal data concerning them be erased and to request that restrictions are placed on the processing of their personal data.

11.2 Any such requests should be forwarded to the Information Manager in order to co-ordinate a response.

12. Information Sharing

12.1 Information sharing occurs when one or more agencies or professionals share information about a data subject for the better provision of a service or where it is in the best interests of that data subject.

12.2 The Council has signed up to the standard for sharing personal data across Staffordshire as part of the 'One Staffordshire' data sharing agreement, and sharing of personal data should comply with this standard.

12.3 Information Asset owners / service managers must ensure that the Information Manager is consulted where a new sharing agreement is being considered.

13. Privacy Notices

13.1 Whenever personal data is collected directly or indirectly from an individual, staff must ensure that a suitable, plain language privacy notice is provided covering all the information required under Articles 13 and 14 of the General Data Protection Regulation.

13.2 These notices will be posted online and will be made available in hardcopy on request. Assistance and guidance on the formulation of these notices can be obtained from the Information Manager.

14. Data Retention

14.1 The Council will retain personal data in line with its legal or business obligations and these are detailed in the Councils Retention Policy and Guidelines.

14.2 All staff and third party's holding Council data should work on the principle of holding data for the minimum time required, and that once no longer needed data is securely deleted or destroyed.

15. Embedding Data Protection within projects

15.1 The Council will apply the principles of data protection by design and by default in all its projects and processes that use personal data. Staff will make sure that new projects involving significant use of personal data (whether internal or using an external third party) are reviewed via the Data Protection Impact Assessment form and process.

15.2 Staff should seek further guidance from the Data Protection Officer and/or Information Manager if they are unsure whether an impact assessment is appropriate. Wherever possible data minimisation should be considered and techniques such as data masking, pseudonymisation or anonymisation should be considered.

16. Contractors

16.1 The Council works with trusted third parties to whom we pass personal data to for processing. Typically, these will be companies that carry out a service on the Council's behalf such as couriers, debt collection agencies and other suppliers.

16.2 Any such disclosures of personal data should be listed within the privacy notices, which are located on the Council's website. We will require all data processors to sign a written contract compliant with Article 28 of the GDPR. Standard terms and conditions can be obtained from Legal Services.

17. Training and Awareness

17.1 All Council staff need to be aware of their, and the Council's obligations under the Data Protection Legislation. A training programme is in place for all staff to ensure they are aware of their obligations under the Data Protection Legislation. Periodic refresher training will be provided to maintain and update staff awareness and knowledge of Data Protection requirements.

17.2 The mandatory training will be supported by a regular programme of communications to staff.

17.3 Managers are responsible for ensuring all members of staff take appropriate data protection training as part of their induction process. It is also a manager's responsibility to arrange any necessary service specific training.

18. Policy Review and Revision

18.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.

18.2 Policy review will be undertaken by the Data Protection Officer in consultation with the Senior Information Risk Owner.

19. Related Legislation and Corporate Policies

19.1 The Council has a legal obligation to comply with the following relevant legislation:

- Data Protection Legislation
- Computer Misuse Act 1990
- Copyrights, Designs and Patents Act 1988
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Private and Electronic Communications Regulations 2003

This list is not exhaustive.

19.2 This policy should be read in conjunction with the ICT Security Policy.

Appendix 1

Glossary

Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed
Data Protection Legislation	Means the General Data Protection Regulation and the Data Protection Act 2018
Data Processor	Any organisation or person (other than an employee of the data controller) who processes data on behalf of the data controller
Data Subject	Means an individual who is the subject of personal data
Personal Data	Any information relating to an identified or identifiable living individual who can be directly or indirectly identified in particular by reference to an identifier.
Processing	Processing in relation to personal data means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:- a) collection, recording, organisation, structuring or storage b) adaptation or alteration c) retrieval, consultation or use d) disclosure by transmission, dissemination or otherwise making available, e) alignment or combination, or f) restriction, erasure or destruction
Sensitive Personal Data	Defined as personal data concerning: racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; sexual orientation or criminal proceedings or convictions.