CANNOCK CHASE COUNCIL

COUNCIL

26TH AUGUST 2009

REPORT OF CHIEF EXECUTIVE

DATA PROTECTION ACT – NEW POLICY

1. Purpose of Report

To seek Council approval for the formal adoption of the 'Data Protection Policy'

2. Recommendation(s)

That Council approves and formally adopts the 'Data Protection Policy'

3. Conclusions and Reason(s) for the Recommendation(s)

Cannock Chase Council has a requirement for a Data Protection Policy to ensure:

- The Council does not contravene the Data Protection Act 1998
- The Council maintains high standards of confidentiality when working with personal information.
- That the Council does not receive bad press for misuse of personal data.

4. Key Issues

This policy lays out how Cannock Chase Council will collect, store, handle and use any personal information it needs to carry out its work. 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 Members and employees of the Council adhere to this policy to ensure that the confidence is maintained in the Council and its handling of personal information.

Failure to follow the guidance and ensure that the Council abides by Data Protection legislation can result in the imposition of penalties upon the Council. The Information Commissioner has the power to bring the prosecutions and if found to be in breach of the Act a Crown Court may impose an unlimited fine. They also have the power to prohibit the Council from processing personal data which would in theory close down many functions of the Council such as those mentioned in section 1.

ENCLOSURE 9.2

REPORT INDEX

Report Author Details: (name, title and extension number)

Section 1

Background

The policy describes how Cannock Chase Council will collect, store, handle and use any personal information it needs to carry out its work. Although this policy will cover all personal information held by the Council, this would include information such as personnel records, personal benefits information and housing tenants information. The policy applies to all staff, Elected Members, contractors, partners and any others working with personal information controlled by the council.

So that we can deliver the services and standards our customers expect, Cannock Chase Council needs to collect and use personal information. The Data Protection Act 1998 requires us to follow certain rules, we must also maintain our own high standards of confidentiality when we work with this information.

Section 2

Details of Matters to be Considered

Responsibility for successful implementation rests with the Chief Executive, Directors, all employees, Leader of the Council and elected members.

The Information Manager will oversee the functioning of the policy and ensure all members and staff are made aware of it. This will be carried out via use of the Council's Intranet, informative emails and training & induction sessions.

The policy recognises that all employees have a vital role to play in the effective implementation of the policy.

Section 3

Contribution to CHASE

To support the organisation's requirement to ensure personal data is handled correctly and to ensure its security, therefore supporting the whole organisation to deliver the CHASE priorities.

Section 4

Financial Implications

Any costs associated with Data Protection are contained within existing budgets.

Section 5

Human Resource Implications

No identified implications

Section 6

Legal Implications

Legal implications are identified throughout the proposed Data Protection Policy.

Section 7

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.

Section 8

Human Rights Act Implications

No identified implications.

Section 9

Data Protection Act Implications

Policy will aid Data Protection Processes. / No Implications

Section 10

Risk Management Implications

Policy will aid Risk Management Processes. / No Implications

Section 11

Equality and Diversity Implications

No Implications

Section 12

Other Options Considered

N/A

Section 13

List of Background Papers

N/A

Annexes

None

Report Author Details

Darren Edwards – Information Manager, PR & Marketing.

Extension 4447.

Data Protection Policy

Cannock Chase Council

May 2009

Purpose and scope

This policy describes how Cannock Chase Council will collect, store, handle and use any personal information it needs to carry out its work. The policy applies to all staff, Elected Members, contractors, partners and any others working with personal information controlled by the council.

In this policy personal information means information relating to a living individual who can be identified from the information itself or from the information when linked to other information we may have or are likely to get. For example a form with no name or address may be personal information if it contains a reference number that we could look up to link it to an individual. Where there is doubt as to whether specific information is covered by this policy the definition of "personal data" in the Data Protection Act 1998 shall be used with due regard to relevant case law.

The Policy

So that we can deliver the services and standards our customers expect, Cannock Chase Council needs to collect and use personal information. The Data Protection Act 1998 requires us to follow certain rules, we must also maintain our own high standards of confidentiality when we work with this information.

The council supports the objectives and principles of the Data Protection Act 1998 and recognises the need for maintaining the confidentiality and integrity of the personal information it holds.

1. The council requires all of its employees, Members, contractors and partners to comply fully with this policy and with all other relevant legislation. For reference the Data Protection Principles are summarised at Appendix 1 and also appear on the Council's intranet.

2. Chief Officers are responsible for compliance with this policy in their directorates. All directorates of the council will nominate at least one Data Protection Representative to liaise with Information Manager on matters relating to data protection and freedom of information.

3. Employees must be aware that they may be exposing the council to legal action or even committing a criminal offence personally if they breach the provisions of the Data Protection Act 1998. Disciplinary action may be taken against any employee who breaches any instruction contained in, or arising from this policy.

4. The council will hold the minimum personal information necessary for its work and the information will be destroyed once the need to hold it has passed.

5. Every reasonable effort will be made to ensure that information is accurate and up-to-date, and that suspected or reported inaccuracies are investigated and, where appropriate, corrected without unnecessary delay.

6. The council recognises that personal information may be confidential and that unjustified disclosure is an offence under the Data Protection Act 1998. All our information systems, manual or automated, which hold personal information will

therefore be specified, designed and operated to allow the council to comply with the Data Protection Act 1998.

7. The council will respect all individuals' rights as provided by the Data Protection Act 1998 and other relevant legislation.

8. Requests for access to information will be handled in line with the Council's procedure for dealing with subject access requests. A Subject Access Request form is attached as Appendix 2. Where an individual requests a copy of information held about them, the information will be provided as long as the request is:

   - in writing;
   - accompanied by sufficient information to assure the council of the individuals identity;
   - accompanied by sufficient information to enable the council to locate the information requested;
   - accompanied by the appropriate fee
   - not subject to an exemption; and
   - within the scope of the currently accepted definition of personal data.

9. Where the amount of work the council has to put in to providing a permanent copy of the information is excessive in comparison with the benefit to the individual in having that copy the council may give access to the information by inspection rather than providing a copy. This can not be used as a reason for denying access, only for providing access by inspection only. This decision should only be made by the Information Manager or the named Data Controller.

10. If complying with a request for access would involve disclosure of information about another person the council will seek the opinion of that person except where exempt from this by the Data Protection Act 1998 or other relevant legislation. If consent is not given the manager responsible for the information and the Information Manager will make a decision as to whether to disclose, partly disclose or withhold the information. The decision will be based on whether or not it is reasonable in the specific circumstances to release the information. A written record of this decision will be kept on file by the Information Manager. Any required advice should be sought from the Information Manager.

    If, in exceptional circumstances, consent of third parties can not be sought a decision will be made as it would if consent were withheld.

11. Personal information will be disclosed only for legitimate purposes, in accordance with the Data Protection Act 1998 and only to:

    - the data subject;
    - any organisation having a legal power to demand disclosure;
    - any organisation having a legal power to receive the information where the council believes it is appropriate and in the public interest to disclose it;
    - any organisation operating under a protocol for information exchange with the council in so far as the protocol and relevant legislation allows the disclosure;

- a third party where appropriate consent has been obtained from the data subject providing it is not believed that the data subject would object to the disclosure;
- a third party who has been given legally responsibility for the data subject providing it is not believed that the data subject would object to the disclosure;
- any other recipient when the council is under the direction of a court order or other notice served on the council by an agency having powers to demand disclosure; or
- any other recipient only where the disclosure is in accordance with the provisions of the Data Protection Act 1998 and other relevant legislation.

12. All computer systems and manual records within departments which contain information about individuals must be identified to the Information Manager and made adequately secure. The Information Manager must be informed of any changes in processing of personal information to allow the council's entry in the public register of data controllers to be kept up to date. All persons covered by this policy have a responsibility to co-operate with this task and must inform the Information Manager of any new work involving personal data or changes to their processing of personal data, such as use for additional purposes. A form is supplied for this purpose – See Appendix 3.

13. Where information is routinely shared with other agencies the process must be fully documented; this may be in a procedure, protocol or sharing agreement. Such disclosures must only be made in accordance with the agreed process. An auditable record of all such disclosures shall be kept.

    The Information Manager must be informed of any such agreements. They must also be informed of any new or revised sharing agreements to enable compliance to be checked.

    For further information please refer to the External Data Transfers Policy.

14. With respect to transferring personal information between departments within Cannock Chase Council, this must be approached on a case by case basis. The Information Manager must be consulted where the transfer of personal information between departments is being considered. This is to ensure that we are not in breach of the second Data Protection principle which provides that Information should not be used for purposes other than that for which it was originally intended / collected.

15. Any non-routine requests for disclosure of personal information should be directed to the Information Manager who will liaise with the appropriate business unit. An auditable record of all disclosures will be kept.

16. Where personal information is being collected from the data subject regardless of the method of collection, the data subject will be given the information in section 18.

17. Where personal information is being collected from a third party regardless of the method of collection, the data subject will be given the information in section 18.

18. The information referred to in sections 17 & 18 is:

- The identity of the Data Controller (Cannock Chase Council);
- All purposes for which the information will be kept or used; and
- Any other information required to ensure information is processed fairly and that the data subject is fully aware of the use to which the information will be put, such as details of further disclosures.

All data collection forms, letters, telephone scripts, electronic forms, emails, etc. will be designed to clearly convey this information to the data subject.

19. No information will be used for any purpose other than those of which the subject is aware, except where this is permitted by the Data Protection Act 1998.

20. In cases where consent is required before personal information is used a record will be kept by the responsible manager of any consent sought, given or refused.

21. Where personal information is stored in manual format, the staff member currently responsible for that information is accountable for its security. This encompasses the requirement for all documents of this nature to be secured whenever the member of staff is not present. In particular at the end of each day all personal data must be locked in a suitable secure location.

22. Where personal information has to be taken off-site, either on an electronic device or on paper, extreme caution must be exercised at all times to protect the information from loss, damage or unauthorised access. In the case of electronic information the Information Manager or Information systems development manager should be consulted to determine if additional controls, such as encryption should be applied. For further information see the Council's External Data Transfers Policy.

23. Where the council is a member of a partnership or part of a multi-agency working arrangement it shall be established at the outset who is the data controller for any personal information collected, used or produced. Appropriate procedures will also be established for handling requests for access to this information from the data subject or any other person or agency. Joint data controller arrangements are permitted; in these cases the responsibilities of each party must be fully documented.

24. In cases where the council hold information as a consequence of providing information processing services to third parties information will only be used in accordance with instructions from that party, except under the direction of a court order or agency empowered in law to demand it. Outside organisations using the council as a data processor or using the council's facilities for its own purposes will be responsible for notification of their systems, along with any other arrangements made in order to comply with the requirements of the Data Protection Act 1998.

25. To ensure the security and integrity of all data held by the authority, no private use shall be made of any equipment belonging to the authority except where granted by any other internal policies such as the
    - IT Security policy.
    - Copyright and Patents Act

- Email and Internet use policy

26. Computer equipment and accessories owned by staff must not be used for any other purpose than Council business – For more in depth detail please refer to the Council's IT Security Policy.

27. All persons covered by this policy must adhere to the Council's Records Management Policy, security policies, related policies, standards and guidelines and must comply with all security advice issued to prevent unauthorised access to personal information and to prevent it from being lost, stolen or rendered unusable.

28. Personal information 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 use of their personal information except under a contract which requires protection equivalent to that provided by European legislation. Contact the Information Manager if you are considering this action.

29. No personal information will be published on any Internet or intranet site without the consent of the data subject except where allowed by current legislation. Where consent is not required the subject of the information will be fully informed and allowed to express their opinion prior to publishing the information.

30. Websites operated by the council will carry an up to date privacy statement which will be observed by any person having access to information collected through the site.

31. Data Destruction – Data should not be held longer than necessary in any form. For guidance on retention timescales contact the Information Manager. The Council's Email policy.

32. Training – All new members of staff will be offered a Data Protection introductory training session. Guidance will be published on the Council's intranet site and also in booklet form. Additional Data Protection awareness sessions will also be run when needed.

33. Additional information relating to the handling and security of data: All employees must be aware of the Council's IT Security Policy, a copy of which is available to download from the Council's Intranet. This policy covers other aspects of data protection such as the positioning of computer screens which display personal information.

34. The registered details of the data controller for personal information processed by Cannock Chase Council is:

Cannock Chase District Council
P O Box 28
Beecroft Road
Cannock
Staffordshire
WS11 1BG

35. Queries relating to Data Protection should be sent to the Information Manager at the above address. All such queries received elsewhere in the council should be forwarded immediately to the Information Manager.

In the event of loss, or assumed loss of data – Escalation Procedure

On discovery or being notified of an individual's personal information has or may have been compromised, the Information Manager must be notified immediately.

1) The Information Manager will notify:

- The relevant Director from which the loss or potential loss originated.
- The ICT Manager.
- PR & Marketing.

2) The Information Manager along with the original member of staff responsible for the data will assess the potential implications for the individual(s) whose information has been compromised and if necessary:-

- Notify the individual concerned,
- Advise the individual of their rights,
- Provide the individual with appropriate support.
- Complete a Police incident report.

If the Information Manager is not available, the ICT Manager must be notified.

Incident Reporting

Council staff, have a responsibility to ensure the security and confidentiality of **all** information.
In the event of a security incident or suspected incident, these must be reported to the Council's Information Manager immediately. If the Information Manager is not available the Council's ICT Manager must be notified immediately.
A security incident is an event that may result in:

- Disclosure of confidential data
- Data degradation/corruption
- Loss of data or equipment
- Unauthorised access
- Financial loss
- Legal action

Incidents should be investigated and resolved with appropriate assistance from ICT.

Revision control

This policy is owned by the Information Manager and will be reviewed and where necessary revised in line with changes to legislation or developments in case law or national guidelines.

Appendix 1

Summary of the Data Protection Principles

These principles apply to any use of personal information from collection to destruction. For the full text of the Principles see the Data Protection Act 1998.

First Principle
Personal data shall be processed fairly and lawfully, Personal data will only be processed where defined conditions are met.

Second Principle
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.

Third Principle
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle
Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

Sixth Principle
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Seventh Principle
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.

Eighth Principle
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.

APPENDIX 2

Subject Access Request Form

(Form on next page, the rest of this page is intentionally blank)

Subject Access Request Form

Under Section 7 of the Data Protection Act 1998, subject to certain exemptions, individuals have the right to access the information about them which we (or a processor acting on our behalf) may hold. To assist us in dealing with a request for such information please complete this form and return it to the Data Protection Officer at the address shown overleaf.

Data Protection Act 1998

1 Please provide the following details about yourself:

Full name

Address

Postcode

Tel No

Fax No

E-mail

2 Are you requesting information about yourself?

If so, you are the data subject and documentary evidence of your identity is required, i.e. driving licence, birth certificate (or photocopy) and a stamped addressed envelope for returning the document.

(Please go to Section 4)

If not, please supply the written consent of the data subject, together with documentary evidence of their identity as above, and supply their details as follows:

Full name

Address

Postcode

Tel No

Fax No

E-mail

3 Please explain why you are requesting this information rather than the the data subject:

Data Protection Act 1998

4 Please describe the information you seek together with any relevant information to help us identify the information you require: (e.g. Rent or Council Tax Reference)

5 ALL APPLICANTS MUST COMPLETE THIS SECTION

(Please note that any attempt to mislead may result in prosecution.)

I confirm that the information given by me on this subject access request form to Cannock Chase District Council is true, and I understand that Cannock Chase District Council may need more information to confirm my identity/that of the data subject and to locate the information that I am requesting.

Signature

Date

6 Please return the completed form to the Data Protection Officer together with :-

a) Evidence of your identity(ies).

b) Evidence of the data subject's identity (if different from (a))

c) Stamped addressed envelope for return of proof of identity and, where applicable, authority document.

d) The fee of £5 (cheque made payable to Cannock Chase District Council) unless you are unemployed, or in receipt of Income Support/Housing Benefit or in receipt of state retirement pension and would qualify for such benefits, in which case no fee is payable.

Employees requesting information on purposes related to employment and Elected Representatives requesting information on purposes related to office of elected representative do not have to pay a fee.

If this is your second or subsequent request of the same purpose within twelve months the fee is £10.

Whilst Cannock Chase District Council must respond to your request for information within 40 days, please note the time period does not run until all of the above has been received.

Return to: **Data Protection Officer,**
Cannock Chase District Council, Civic Centre, PO Box 28,
Beecroft Road, Cannock, Staffs. WS11 1BG