CANNOCK CHASE COUNCIL

COUNCIL

25 AUGUST, 2010

REPORT OF CHIEF EXECUTIVE

RESPONSIBLE PORTFOLIO LEADER(S) – LEADER OF THE COUNCIL

EXTERNAL DATA TRANSFERS – NEW POLICY

1. Purpose of Report

1.1 To seek Council approval for the formal adoption of the 'External Data Transfers Policy'

2. Recommendation(s)

2.1 That Council approves and formally adopts the 'External Data Transfers Policy'

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

3.1 Cannock Chase Council has a requirement for an External Data Transfers Policy to ensure that:

- The Council does not contravene the Data Protection Act 1998
- The Council maintains high standards of confidentiality when transferring personal information out of and into the organisation.
- That the Council does not receive bad press for loss of personal data.
- The confidentiality of its residents' information is not compromised.

4. Key Issues

4.1 The Council is regularly approached to share data it holds with others either for partnership working, external processing or for data matching exercises, such as our benefits department sharing information with the Department of Work & Pensions. Cannock Chase Council must ensure the security of this data whilst it is being transferred and take great care to ensure public confidence is maintained regarding any information we hold, process or share with other partner organisations e.g. other public bodies. Elected Members and employees also have individual legal responsibilities under the Data Protection Act 1998, i.e. to ensure personal information with which they work, is handled correctly and in a secure manner.

4.2 There have been many incidents reported in the press both locally and nationally regarding loss of public data, such as the recent occurrence of a memory stick containing personal data that was accidentally left at a public house in Cannock. In addition to the Council ensuring that its residents' and partners' data is secure, the Council wishes to avoid damage to its reputation by negative PR or press coverage.

4.3 The objective of this policy is to establish and maintain the security and confidentiality of information shared with our external partners:

- Ensuring that all Elected Members and employees are aware of external data transfer procedures.
- Outlining the principles of security and explaining how they will be implemented.
- Introducing a consistent approach to transfers, ensuring that all Elected Members and employees understand their own responsibilities.
- Supporting a level of awareness of the need for Information Security as an integral part of day to day business.

4.4 It is essential that Elected 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.

REPORT INDEX

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

Section 1

Background

There has been much made in the media recently regarding the loss and theft of public data. These incidents include the loss of memory sticks, CDs and Laptops containing confidential information held by the public sector.

The Council is regularly approached to share data it holds with others either for partnership working, external processing or for data matching exercises.

The objective of this policy is to establish and maintain the security and confidentiality of information shared with the Council's external partners. The Council must take great care to ensure public confidence is maintained regarding any information we hold, process or share with other partner organisations.

Section 2

Details of Matters to be Considered

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

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 could, in theory, close down many functions of the Council, for example Revenues & Benefits and Housing.

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

The policy recognises that all employees and elected Members 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 organisation in the delivery of 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 Council's Data Protection Policy and within the proposed External Data Transfers 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.

Cannock Chase Council

External Data Transfers Policy

Cannock Chase Council

June 2010

Beacon Authority

2004-2005
Crime and Disorder Partnerships

2005-2006
Healthy Communities

2006-2007
Transforming the Delivery of Services Through Partnerships

Document Details	
Title:	External Data Transfers Policy
Author:	Darren Edwards
Date Created:	
Last Saved By:	Darren Edwards
Last Saved:	04 June 2010
Filename:	

Documentation Control			
Version	**Date**	**Reason for Issue**	**By**
v 1.0	22/10/2009	Document created	Darren Edwards
v 2.0	15/03/2010	Amended references to IT security standards.	Darren Edwards

Documentation Approval			
Name	**Role**	**Date**	**Signature**

Documentation Review		
Name	**Role**	**Date To Review**
Darren Edwards	Information Manager	1 March 2011

Distribution List		
Name	**Division**	**Job Title / Department**
Darren Edwards	PR & Marketing	Information Manager
Kathryn Cooper	PR & Marketing	PR & Marketing Manager
Tan Ali	ICT	ICT Services Manager
Colin Buckler	ICT	ICT Technical and Development Mgr
Stephen Baddeley	Audit	Chief Internal Auditor

Purpose

The protection of information that the Council holds, particularly about those who use our services is vital. Elected members and employees must take all necessary steps to prevent unauthorised access to it.

The Council is regularly approached to share data it holds with others either for partnership working, external processing or for data matching exercises. We must ensure the security of this data whilst it is being transferred. We must take great care to ensure public confidence is maintained regarding any information we hold, process or share with other partner organisations e.g. other public bodies. Elected members and employees also have individual legal responsibilities under the Data Protection Act 1998.

In addition more and more use is being made of portable equipment or media devices to work on information off site and as such individuals need to be take steps to ensure the security of information stored and access to it.

Policy Objective

The objective of this policy is to establish and maintain the security and confidentiality of information shared with external partners of the Council inclusive of:

- Ensuring that all members and staff are aware of external data transfer procedures.
- Describing the principles of security and explaining how they will be implemented.
- Introducing a consistent approach to transfers, ensuring that all members and staff understand their own responsibilities.
- Supporting a level of awareness of the need for Information Security as an integral part of day to day business.

Council managers are responsible for ensuring that their permanent, temporary staff and contractors are aware of this policy, the Data Protection Policy, the IT Security Policy and

- Personal responsibilities for information security are communicated, ensuring that all staff receive appropriate levels of education and training in this area.
- Know how to access advice on information security matters and how to report incidents using the correct procedures.

Scope

All Transfers of data in and out of the Council are subject to this policy and the Data Protection Act 1998, excluding:

- Any information that is generally available to the public.
- Any information that could be released under the Freedom of Information Act 2000.

The ICT Security Policy should be referenced alongside this policy.

If unsure of the scope of this policy please refer to the Information Manager.

Available assistance and guidance

If you have any questions regarding this policy or any item within or require further advice/guidance or training then please contact the Information Manager.
If you have specific questions regarding ICT Security or data encryption please see the ICT Security Policy or contact the ICT Security Officer.

A Data Protection guidance section also exists on the Council's Intranet and a quick reference is attached as Appendix D.

Data Protection training is available via the Information Manager or Training Officer.

Roles and Responsibilities

- The policy aims to ensure that all Members, employees and those whom we transfer data to, are aware of their information security responsibilities. Information security is a shared responsibility. Confidentiality, integrity and availability of information could be compromised due to a breach of security (which could be accidental or malicious).
- Each Member and employee should be reminded that they are personally responsible for ensuring that no breaches of information security result from their actions.
- Failure by individuals to apply controls particularly in handling personal data that does lead to a breach could amount to gross misconduct depending on the circumstances. This includes the loss of devices holding personal data or the loss of personal data transmitted electronically or by post/courier.
- Personal Data should always be encrypted and transmitted electronically wherever possible as this is a more secure method.
- Recipients of our data should give us assurances that they will handle our data to or above our standards. We should also ensure that recipients have the right to receive and process our data.
- Roles and responsibilities should be documented fully

References and guidance to 'Employees' within this document also apply to contractors.

Data received should not be used for any purpose other than specified.

The Information Manager must always be notified of any new instances whereby data is to be transferred outside the organisation (where covered by this policy; see Scope) - Particularly in cases where the transfer is to be on a regular basis, even if, for example, this is only once a year. This is to allow us to add your transfer type to the corporate data transfers register.

Electronic Data Transfer Methods & Guidance

Information sharing across Council and non-Council environments is becoming a more and more common requirement. Transmitting information by electronic means exposes that information to a risk of unauthorised access and corruption during transmission.
ALL transfers of electronic data (see scope) transmitted externally must be subject to encryption, password protection and be at least compliant with current ICT Policies. For further information on passwords to ensure adequate security, the ICT security policy should be consulted. Should any employee require file encryption and password protection ICT services will assist or carry out this function on your behalf. Recipients of our data should be contacted by us to arrange password transfer and decryption of sent data. We should never accept a call requesting the password. The relevant member of staff should always be completely satisfied that the recipient of the data is the intended and authorised recipient.
Data transferred should be the minimum amount necessary for associated work to be completed; As per the 3rd principle of the Data Protection Act 1998.
Those responsible for transferring data should also be reminded that extracts from systems should be held securely before / after transfer. For example a dedicated folder / storage area should be used with limited permissions.
Consider using .pdf converting software if data to be sent to external / 3 party is not to be re-processed. The same can apply to data received.

Information / Data should ONLY be sent

- After the approval by a relevant manager.
- When the Information Manager is aware of the transfer (notification by email only to 'infomanager' (internal) / infomanager@cannockchasedc.gov.uk)
- Assurances that the recipient will handle the data in accordance with our security guidelines have been received. The Data Transfer Log (Appendix C) must be used.

Sending Information via Email

All information covered by this policy, electronically transmitted externally via email must be subject to encryption, password protection and be at least compliant with current ICT Policies.
The Councils standard email and internet system on its own DOES NOT meet this requirement and MUST NOT be used to transmit personal information. Please contact the ICT Service Desk if you require assistance in transmitting sensitive information.
In addition,

- Always use the Council email disclaimer, this is automatically added to outgoing email. (If in doubt contact ICT for guidance)
- Use minimum amounts of information in email, if individuals can be referred to by reference numbers (such as complaints or information requests) this should be the preferred option.
- Ask the recipient to confirm receipt and record this on the data transfer log (Appendix C)
- Follow up any none-response within 1 working day.

The exception to this rule is where the recipient is the data subject and has requested that we send their data via email. An example of this is where a resident has requested that we send their Council tax bill via email.

Any email containing personal information should be deleted as soon as it is no longer required. This may be as soon as an email has been sent. It should be remembered, dependant upon how an individuals mail account is set up, that on deleting an email, it will then appear in 'deleted items', where it must also be deleted from to remove it completely from the email system.

Refer to the Council's Email Policy or contact ICT for further information on this subject.

Media in Transit

All personal information sent out externally via electronic media must be subject to encryption, password protection and be at least compliant with current ICT Policies.

- Follow guidance in the sections below relating to Removable media.
- Confirm the name, department and address of the recipient.
- Seal the information in a robust envelope.
- Add details of the sender and data content – security information MUST not be included
- Mark the envelope 'Private and Confidential – to be opened by Addressee Only.'
- When not transporting the data personally, trusted Couriers should be used. A list of approved couriers can be obtained from Support Services.
- Post should not be used as a method for transferring sensitive or personal data; it may be possible to provide more secure electronic transfer methods such as SFTP. The IT Security Officer can offer advice and support in relation this.
- Ask the recipient to confirm receipt and record this on the data transfer log (Appendix C)
- Follow up any no response within 1 working day.

Removable Media - USB Memory Sticks & Drives (including mobile phones with data storage)

When Transferring data via Memory stick - all information covered by this policy must be subject to encryption, password protection and be at least compliant with current ICT Policies.

These are useful devices as they are of high capacity, small, transfer data quickly and are easily used in machines with compatible connectors. However they present a high risk. Therefore special care is required to reduce the risks associated with memory sticks.

- Any memory stick used in connection with council equipment or the network must be supplied by and registered with ICT. These devices have security features that must be used.
- Many memory sticks cannot be password protected and may bypass the virus and malware checking software. Such devices must not be used.
- Memory sticks brought in from home must never be used.
- Memory sticks from other organisations should be checked by ICT before being used on any Council equipment
- As a large amount of data can be stored on a memory stick care should be taken over what data is transferred onto such devices. Only the data that is authorised and necessary to be transferred should be saved on to the device.
- Due to their small size there is a higher risk of the memory stick being mislaid or lost and a risk of the memory stick being damaged. Therefore special care is required to physically protect the memory stick and the data.

- Anyone using a memory stick to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Virus and malware checking software must be used when the memory stick is connected to a machine.
- Memory sticks are not to be used for archiving or storing records as an alternative to other storage equipment. Data of this nature should be held on secure Cannock Chase Council network areas apart from where authorised by ICT.
- Data on memory sticks must be completely removed as soon as its storage on the stick becomes no longer absolutely necessary.
- Data that has been deleted can still be retrieved. Formatting the memory stick is the only way to remove data. Contact ICT for advice.
- If a USB memory device has been sent to an external recipient, the member of staff responsible for the transfer must ensure the data has been received by the correct person. Any non response should be followed up within 1 working day.

Removable Media – Recordable Compact Disks / DVD's / Floppy Disks

When Transferring data via Removable media - all information covered by this policy must be subject to encryption, password protection and be at least compliant with current ICT Policies.

Disks are of high capacity, small and are easily used. Unfortunately they present a high risk. Therefore special care is required to reduce the associated risks.

- Only data that is authorised and necessary to be transferred should be saved on to the media. The files should be password protected and encrypted if they are taken outside of council buildings.
- Anyone using a CD, DVD or diskette to transfer data must consider the most appropriate way to transport the media and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Storage of data on a CD, DVD or diskette is a snapshot of the data at the time it was saved to the media. When using this method to store data, adequate labelling must be undertaken facilitating easy identification of the version of the data as well as its content.
- Appropriate security and storage methods should be applied to the media so that this business asset is protected.
- Disks from any external source should be checked by ICT before being used on any Council equipment.
- As a large amount of data can be stored on a disk, care should be taken over what data is transferred onto such devices. Only the data that is authorised and necessary to be transferred should be saved on to the device.
- Due to their small size there is a high risk of a CD / DVD / diskette being mislaid or lost and a risk of damage. Therefore special care is required to physically protect the disk and the data.
- These types of device should not be used, by business users, for archiving or storing records as an alternative to other storage equipment. Data of this nature should be held within the network areas provided.
- Virus and malware checking software must be used when the disk is placed in a Council machine.

For Further information please refer to the ICT Security Policy.

Sending Information via Facsimile

No personal information should be sent via fax. Fax is a very insecure method of transferring data and has no associated method of security.

FTP Transfer / http:// or uploading to a 3rd party website

File Transfer Protocol allows a user to 'upload' or transfer data from one computer to another but is not a secure method of data transfer. In the Council's context this usually involves uploading a file directly from a workstation to a remote site, usually accessed via a web browser or FTP software. If this method is to be used the file being sent should be encrypted, password protected and it's security be at least compliant with current ICT Policies. ICT should also be consulted on the use of such systems.

Requests for Information over the Telephone – Guidance

Information conveyed over the phone should generally only occur as one off pieces of data or information, perhaps to confirm an identity for example.
Any greater amount should always be sent via another secure form of transfer method, such as those mentioned in the above sections.

Information should only be given over the telephone where a current agreed procedure is in place and / or authorisation from a relevant manager has been sought. As a minimum requirement for this procedure the following must be observed:

- Confirm the details of the requester – e.g. name, job title, department and organisation of the person requesting the information.
- Confirm the reason for the information request if appropriate
- Take a contact telephone number (never a direct line or mobile telephone number).
- Check whether the information can be provided.
- Check with your manager if you can disclose this information.
- Call the requester back with the information and ensure that you are talking to the person entitled to receive that information.
- Provide the Information only to the person who has requested it (do not leave messages either with a person or answer machine)

Ensure that you record your name, date and the time of the disclosure, the reason for it and who authorised it. Also record the recipients name, and where appropriate; job title, organisation and telephone number. Use the data transfer log to assist (Appendix C).

Data being Collected from Council Premises

The above procedures mostly assume that data is being sent off site by us. Where suppliers or other recipients of data are visiting Council premises to collect data, the data must be signed for by the recipient only after the member of staff handing over the data is entirely satisfied that that person is the authorised recipient. This must be confirmed by proof of ID on the recipient's part.

In cases where data is being transferred externally by other means not mentioned above, please contact the IT Security Officer for advice.

Incoming Data Transfers

Just as it is important that data transfers outwards should be strictly controlled and accounted for, incoming data should also be monitored.
On acceptance of the data it is necessary that the member of staff responsible for the system on which the data is being held, and whom is receiving the data will :

- Take full responsibility for the security of the information which we receive.
- Ensure that only the relevant members/staff have access to the data. For example ICT may be able to provide a restricted folder on the network.
- Ensure that the data is not copied/duplicated for any reason other than stated. Avoid forwarding data onwards through the internal mail system –folders / restricted user permissions should be employed to minimise risk of data being passed to unauthorised members of staff.
- Ensure that any data that is provided is destroyed when the specified work has been completed.
- Agree to inform the Information Manager.

Upon receiving data, an 'Data Transfer Log – Incoming Data' form must be completed and forwarded to the Information Manager (Appendix D).
These forms may be used for one-off data transfers or for a series of regular transfers.

Individual User Roles and Responsibilities for Data Transfers

Each department responsible for the transfer of personal data in or out of the organisation should have a formal documented procedure in place which can be referred to in the event of absence of the members of staff responsible for the data transfer.
Such procedures will be ideally held by the service manager.

The procedure should include at a minimum, all of the elements contained in either:
for outgoing data;
Appendix C;
'Departmental Personal Data Transfer Procedures – Outgoing Personal Data'

Or

for incoming data;
Appendix D;
'Departmental Personal Data Transfer Procedures – Incoming Personal Data'
For incoming data

The procedure should be completed and retained by the relevant service manager for the duration of the actual transfer of data plus 3 years for audit trail purposes.

In the event of loss, or suspected loss of data or unauthorised access

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 will be investigated and resolved with appropriate assistance from ICT and Audit.

Escalation procedure

On discovery or being notified that a loss or assumed loss of data has occurred, particularly in the case of an individual's personal information, the Information Manager must be notified immediately.

1) The Information Manager will notify:
   - The relevant Director and Head of Service from who's remit the loss or potential loss originated.
   - The ICT Manager / Security Officer.
   - PR & Marketing.
   - Audit

2) The Information Manager along with the original member of staff responsible for the data will assess the potential implications of the loss. In the case of personal data, for the individual(s) whose information has been compromised the Information manager will, 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.

Data held on the Council's Email system

Data, particularly personal data, should not be held on the Council's email system longer than totally necessary. Data should be downloaded or forwarded where appropriate and deleted from the email system. For full guidance see the Council's Email Policy.

Data sharing / Transfer contracts / Agreements

Data sharing contracts and agreements are the responsibility of the department owning / transmitting the data, and before any data is shared:

- A contract / agreement should be drawn up between the department responsible for the data and the recipient.
- Appendix B should be referred to, observing the inclusion of standard clauses stated therein.
- The Council's Legal team should also be consulted to ensure the final contract is correct.

An example of a data sharing agreement / contract can be found in Appendix B.

All data sharing contracts should be copied to the Information Manager for reference.

Corporate Standard for External data transfer.

Can be found in Appendix A.

Using data to test new systems or system upgrades.

Any data used for testing new software systems or systems must not be identifiable personal data. Any data used for these purposes must be completely anonymised. This would involve such as removing real names and if possible NI Numbers and dates of birth.
As per our data protection policy, The Information Manager should be made aware of all systems being used to store personal data within the Council. Any new systems holding personal data should also be registered with the Information Manager including systems in the testing phase.
For additional guidance on this matter please contact the ICT team. Or Information Manager.
For additional guidance on this matter please contact the ICT team.

APPENDIX A

Corporate Standard for External Data Transfer

This entire External Data Transfers Policy constitutes our data transfer standard and therefore must be taken into consideration before the transfer of any data from the Council. In particular, the following pointers must be observed and used as a minimum standard for the transfer of Council Data:

All who transfer data must remember that they are responsible for information security and may be held personally responsible for loss of data.

- Notify the Information Manager of any new instances whereby data is to be transferred outside the organisation - Particularly in cases where the transfer is to be on a regular basis, even if, for example, this is only once a year.

- In the case of personal data transfer, a 'receipt' for data transmitted must be obtained by the member of staff responsible for sending the data. This can be in the form of an email, which will provide proof of receipt for the sender. A record must be made kept of the receipt on the Outgoing data transfer Log (Appendix C).

- Where a receipt is not received the recipient must be contacted immediately. In the case of a courier, they should be contacted to attempt to discover the location of the data. In any case where a loss, or suspected loss of data has occurred, the Incident Reporting procedure in this policy must be observed immediately.

- A contract / agreement must exist between Cannock Chase Council and any recipient of personal or sensitive data. An example of such a contract / agreement can be found in Appendix B.

- Protect "personal" information or confidential business data that needs to be transmitted to external organisations or individuals by, for example, 'zipping' the contents and applying an appropriate password. Encryption techniques and password protection must be used and be at least compliant with current ICT Policies. (ICT can advise on the appropriate methods of encryption).

- Record sensitive data transfers made with reasons, security applied, recipients, dates and acknowledgements. This information must be provided to the Information Manager at the time of the transfer to be logged centrally.

- Always use an approved courier service when physically transferring data. Post should not be used as a method for transferring sensitive or personal data. It may be possible to provide more secure electronic transfer methods such as SFTP. The IT Security Officer can offer advice and support in relation this.

- Protect any sensitive data extracts to memory sticks appropriately. Encryption techniques and password protection must be used and be at least compliant with current ICT Policies. Management approval must be obtained. Where necessary consult the IT Security Officer.

- Keep any equipment or storage media containing data safe in transit (PCs, PDAs, memory sticks CDs) - Personally carry equipment when on board public transport and again Encryption techniques and password protection must be used and be at least compliant with current ICT Policies.

- Immediately report any loss or theft of computer equipment e.g. laptops, PDAs CDs/memory sticks containing Council Data to your Head of Service, The Information Manager, ICT, Internal Audit, the Insurance Section and the appropriate authorities (e.g. British transport police, local police, hotel security, etc.)

APPENDIX B

Example Data Sharing Agreement

All instances of data sharing whereby Cannock Chase Council intend to transfer personal or business sensitive data out of the organisation to another organisation / individual / recipient should include the wording below. The legal team should also be consulted before any such contract / agreement is in place or finalised.

Please note that all references to "partner" in the below sections relate to a recipient of Council data.

Data Protection

1.1 Where appropriate the Recipient of data (the 'Recipient') shall register and maintain registration under the Data Protection Act 1998 as may be amended from time to time and treat any relevant data in accordance with the said Act.

1.2 Without prejudice to the above clause the partner shall at all times comply with the requirements of the Data Protection Act 1998.

1.3 The Partner shall indemnify the Council in respect of any losses claims actions damages or costs arising from the Partner's breach of clauses 1.1 or 1.2 above.

Confidential Information

2.1 The Recipient agrees at all times to treat all Confidential Information as secret and confidential to the Council.

2.2 The Recipient shall not, save for in consequence of clause 2.3, at any time, for any reason, disclose or permit to be disclosed to any person any Confidential Information and the Recipient shall not otherwise make use of or permit any use to be made of any Confidential Information by any third party.

2.3 Confidential information may be released pursuant to the requirements of access to information legislation which includes but is not limited to the Freedom of Information Act 2000 and the Audit Commission Act 1998. Though any such information must only be released through Cannock Chase Council.

2.4 Where required the Recipient shall offer all reasonable assistance to the Council in the Council's compliance with the various requirements of access to information legislation.

2.5 Both parties acknowledge the duties and obligations placed upon the Council by access to information legislation and the Council agrees as far as practicable to exercise its reasonable endeavours in affording the Recipient the opportunity to comment in advance of any disclosure(s) of information as a consequence.

2.6 Should the Council receive a Freedom of Information act 2000 request requesting disclosure of information relating to this Agreement the Council agrees as far as is practicable to refer to items identified by the Provider as being commercially sensitive.

2.7 The Council also, as far as practicable and without fettering its discretion, will notify the Provider of any information it intends to disclose. The Provider may make an application to a court of competent jurisdiction for an injunction to prevent disclosure.

2.8 Save in respect of a timely and appropriate application to a court of competent jurisdiction to prevent disclosure of information by the Council, the Provider agrees to indemnify the Council in respect of all claims which may directly arise as a consequence of any act of omission or commission by the Provider, which prohibits or delays the Council complying with its legal obligations pursuant to access to information legislation.

2.9 On termination of this Agreement (however such termination may arise) the Provider shall deliver up if so required to the Council all working papers, computer disks and tapes or other material and copies provided or prepared by it pursuant either to this Agreement or to any previous obligation owed to the Council regarding the Project.

Data Security

All personal information sent out by us via electronic methods will be subject to encryption, password protection and be at least compliant with current ICT Policies. The recipient will have in place resources to access this encrypted data.

The recipient will also have in place systems ensuring that data supplied by us is held securely and is only accessible by personnel who are required to access or process this data.

Retention

A reasonable period for retention of data must be agreed – individual discussion should take place between the recipient and Cannock Chase Council to determine the appropriate retention period for all / any data transferred. After such time the data will be securely destroyed by the recipient, who will then inform Cannock Chase Council that this has been carried out.

APPENDIX C

Data Transfer Log – Outgoing Personal Data

To be used in instances of Personal Data Transfer FROM Cannock Chase Council TO an External destination. No files are to be sent off site unless it can meet ALL of the following criteria:

- Abide by CCDC IT security Policy
- All aspects of the Data Protection Act are complied with.
- All aspects of the Copyright and Patents Act are complied with.
- The recipient of the information is entitled to hold/view/process the information.
- The files only contain the data that is required – fields that are not required must be removed.
- Any sensitive or non essential data should be redacted/deleted prior to encryption.
- If data is being used for testing purposes NO live data should be used.
- The data is encrypted with a strong password. Minimum of 8 characters long and must include an uppercase, lowercase, number and an unusual character (one of: !£$%^#[]{}).
- Passwords are communicated verbally with the authorised recipient of the data.
- If the filenames contain sensitive information then these need to be compressed into a single file prior to encrypting.

If you have any queries regarding Data Security, please contact the IT Security Officer on ext 4393.

Fully complete the following log, and once completed forward to the Information Manager and the IT Security Officer:

Send To (Name and Company):	
Data Requested to be sent: (and Location of data requested – in case of need to re-send)	
Reason for Sending:	
Method Used to Send:	
Date sent : Frequency (if applicable)	First sent: / / Received: / / Data is sent every : (e.g. 1st of each month) Last transmission : / /
Files Encrypted & by what method?	Yes / No Method:
Retention period; When will data be destroyed?	
Proof of destruction; What proof will be sent.	
Authorised (Service Manager):	User: Date: / /
Receipt received from recipient	Date: / / Format : (e.g. email)

Signed (Information Manager or IT Security Manager):	Date: / /

APPENDIX D

Data Transfer Log – Incoming Personal Data - Checklist

To be used in instances of Data Transfer FROM an External Source to Cannock Chase Council.
By signing this form you agree to:

- Take full responsibility for the security of the information.
- To ensure that only the people named below have access to the data.
- To ensure that the data is not copied/duplicated for any reason other than stated below.
- To ensure that any data that is provided is destroyed when the specified work has been completed.
- That you agree to inform the Information Manager and/or IT Security Manager
- Abide by the Council's IT security Policy and Data Protection policy

If you have any queries regarding Data Security, please contact the IT Security Officer by telephoning ext 01543 4644393.

Please ensure that this form is returned to the Information Manager and IT Security Manager.

Sent From (Name and Company):	
Data Received, Description:	
Method sent by: (e.g. email)	
Date Received : Frequency (if applicable)	First sent: / / Received: / / Data is sent every : (e.g. 1st of each month)
How / where will the data be stored:	
Who will be accessing the data:	
Retention period; When will data be destroyed?	
Proof of destruction; What proof will be sent.	
Authorised (Service Manager):	User: Date: / /
Receipt sent to sender	Date: / / Format : (e.g. email)

Signed (Information Manager or IT Security Manager):	Date: / /