1. INFORMATION SECURITY POLICIES

Submitted by: **Executive Management Team**

Portfolio: **Finance and Budget Management**

Purpose of the Review

To advise the Committee of any staffing matters arising from the annual review of the council's current information security policies and also in relation to a new 'Data Transfer Policy and Procedure'.

Recommendations

(a) That the summary of amendments made to existing policies (Appendix A) be noted.

(b) That the draft Data Transfer Policy and Procedure (Appendix B) be endorsed, subject to the minor amendments set out in the report below being incorporated.

1. Background

1.1 As part of the annual review process of the council's Information Security Policies, recommendations made following a recent external review regarding PCI (Payment Card Industry) compliance were considered and have been subsequently incorporated, where appropriate, to enhance the policy suite.

A summary of the amendments made is attached at Appendix A.

The amendments were discussed at a meeting of the Chair of the Employees Consultative Committee, the Head of Human Resources and the trade unions on 29 January 2013. The trade unions did not indicate that they had any concerns or issues regarding the amendments but they have requested that, in future, any proposed changes to existing policies be highlighted when circulated for discussion.

The suggestion has been noted and will be acted on by your officers.

1.2 A draft 'Data Transfer Policy and Procedure' is attached at Appendix B. This was also discussed with the trade unions on 29 January 2013. At the meeting, the trade unions raised the following points:

- Section 6.1, paragraph 3 (highlighted in bold)
  - The words *'or by post/courier'* should be deleted

- Appendix A – Media in transit section, – bullet point 8 (highlighted in bold)
  - The words '*post should not be used'* to be replaced with '*post will not be used''*

- Relevant employees should receive briefings to ensure they understand their roles and responsibilities

1.3 Section 6.1 relates to the failure to apply adequate controls. The intention is not for employees to be disciplined for errors/omissions made by third parties. It is therefore suggested that the last sentence should read:

'This includes the loss of devices holding personal data, or the loss of personal data transmitted electronically, or the loss of data by post or courier where a more secure method of transferring the personal data should have been selected.'

1.4 The amendments made to the existing policies and the draft Data Transfer Policy and Procedure were considered at the Employees Consultative Committee at its meeting on 18 February 2013. The Committee resolved to endorse the action proposed in relation to Section 6.1 of the Data Transfer Policy and Procedure.

2. Issues

2.1 In order to ensure the council's information security policies remain effective and fit for purpose, it is essential that they are reviewed regularly and additional policies and procedures developed as appropriate.

2.2 It is also essential that relevant staff understand their responsibilities and obligations when handling data and are aware of the potential consequences for both the council and themselves of lapses in data security.

3. Legal and Statutory Implications

3.1 The council is required to comply with The Data Protection Act 1998.

4. Equality Impact Assessment

4.1 The council's information security policies apply equally to all employees.

5. Financial and Resource Implications

5.1 Breaches of the Data Protection Act can result in local authorities incurring significant fines from the Information Commissioner's Office.

6. Major Risks

6.1 See 5.1 (above).

7. **List of Appendices**

Appendix A	Annual Review of Information Security Policies – November 2012 Summary of Amendments
Appendix B	Draft Data Transfer Policy and Procedure

Annual Review of Information Security Policies – November 2012

SUMMARY OF AMENDMENTS

Computer, Telephone and Clear Desk Policy

- Now called the Computer, Telephone and Password Policy;
- Addition of Council's required password default requirements i.e. Change every forty two days, **minimum of** eight alpha-numeric characters in length and not one of twenty previous passwords;
- Shared user IDs should not be used;
- Only when a business need and **with** prior advice from ICT should business calls be made and received **using council issued equipment**, whilst abroad; and
- Screens will automatically lock, however this should not be relied upon and staff should ensure they do this manually.

Remote Working Policy

- **PCs or Laptops** and software must only be provided by the Council, *unless the method of remote access requires users to utilize their own personal computer.* ***In this instance, ICT will provide secure access devices (currently Becrypt sticks);***
- Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Council may recover the costs of repair *calculated at a rate predetermined during an annual review;*
- As with screens based within Council buildings, it should also be ensured that casual 'shoulder surfing' or people overlooking the data on screen does not occur whilst working remotely;
- Approval should be obtained from the relevant Head of Service for the use of the Council's remote access service as well as removable and portable media. Access to these require authentication using a user ID and password; and
- Any remote access that has remained inactive for 30 minutes should automatically sign out to ensure the security of information.

Software Policy

- Before installing a new system onto the network it must be ensured that the defaults provided by the vendor are changed. This includes passwords, SNMP, community strings and unnecessary accounts. This is also applicable in respect of any wireless environment*;*
- Software passwords should be in line with the Corporate Policy;
- Access to all systems should be restricted, and only where a job role requires access in order to perform the role should this be granted. This need for access should be formally granted by an appropriate senior employee such as Head of Service or Business Manager. It should be ensured that this access is documented;
- All user IDs should initially be set to 'deny all' access, with only certain elements activated based upon the job role and formal approval. This ensures that only necessary access is granted; and
- Access can be granted to vendors where necessary. It should however be ensured that this access is disabled when no longer necessary. Whilst enabled it should be ensured that monitoring of the access is undertaken. It

may also be appropriate that vendors may access our systems remotely, but again it should be ensured that this is disabled when not required.

Information Protection Policy

- It should be ensured that unprotected Primary Account Numbers (PANs) are not sent to recipients by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.);
- In addition, for those users who have access to individual cardholder data the individual departments challenge procedure should be complied with in full to ensure the security of both the card data and account details.
- Any technology connected to card payments must be stored in a secure environment;
- Compliance with the Council's External Data Transfer policy; and
- At a minimum the risks in respect of PCI compliance should be considered on an annual basis in line with the Council's Risk Management policies and procedures.

Email Policy

- Incorporated Government Protective Marking Scheme guidance.

Human Resources Information Security Standards

- No amendments.

Legal Responsibilities Policy

- No amendments.

Internet Acceptable Usage Policy

- No amendments.

Removable Media Policy

- No amendments.

Information Security Incident Management Policy and Procedure

- No amendments.

APPENDIX B

NEWCASTLE UNDER LYME BOROUGH COUNCIL

Policy Document

DRAFT - Data Transfer Policy and Procedure

November 2012

Document Control

Organisation	Newcastle-under-Lyme Borough Council
Title	Data Transfer Policy and Procedure
Author	Stephen Heppell
Filename	X:\NULBC Policy Pack\Data Transfer Policy and Procedure.doc
Owner	Audit Manager / Head of Customer and ICT Services
Subject	Information Security Policy
Protective Marking	Unclassified
Review date	November 2013

Revision History

Version	Revision Date	Reviser	Previous Version	Description of Revision
1.0	01/12	S Heppell	-	Initial NuLBC draft
1.1	09/12	S Heppell	1.0	Draft Comments Update
1.2	11/12	S Heppell	1.1	Final Comments

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Information Security Group		
Executive Management Team		
Cabinet		

Document Distribution

This document will be distributed to:

Information Security Group
Executive Management Team
Cabinet
All Employees
All Members

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Cannock Chase Council
- FIT Business Solutions

1 Policy Statement 4
2 Purpose 4
3 Scope 4
4 Definition 4
5 Risk 5
6 Applying the Policy 5
6.1 Roles and Responsibilities 5
7 Policy Compliance 6
8 Policy Governance 6
9 Review and Revision 6
10 References 6
11 Key Messages 7
Electronic Data Transfer Guidance 8
Sending Information via Email 8
Media in Transit 9
Removable Media – Recordable Compact Disks / DVD's / Floppy Disks 10
Sending Information via Facsimile 11
FTP Transfer / http:// or uploading to a 3rd party website 11
Requests for Information over the Telephone – Guidance 11
Transfer of Data Held in Manual Form 12
Data being Collected from Council Premises 12
Incoming Data Transfers 12
Individual User Roles and Responsibilities for Data Transfers 13
In the event of loss, or suspected loss of data or unauthorised access 13
Incident Reporting 13
Escalation procedure 14
Data held on the Council's Email system 14
Data sharing / Transfer contracts / Agreements 14
Corporate Standard for External data transfer 15
Using data to test new systems or system upgrades 15
Appendix B 16
Corporate Standard for External Data Transfer 16
Appendix C
Example Data Sharing Agreement 17
Appendix D 19
Data Transfer Log – Outgoing Personal Data 19
Appendix E 20
Data Transfer Log – Incoming Personal Data 20

1 Policy Statement

Newcastle-under-Lyme Borough Council will ensure that every user is aware of, and understands, the acceptable use of information held by the Council and the need to transfer this information securely.

2 Purpose

The protection of information that the Council holds, particularly that which is personal and sensitive to 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 take steps to ensure the security of information stored and access to it.

This policy aims to establish and maintain the security and confidentiality of information shared with external partners of the Council.

3 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 would be required to be disclosed under the Freedom of Information Act 2000.
- Any information that would be required to be disclosed by the Environmental Information Regulations 2004

The Information Security Policies should be referenced alongside this policy.

4 Definition

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 Act, the Information Security Policies and for ensuring that:

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

5 Risk

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix A.

6.1 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. The roles and responsibilities should be documented fully.

Any reference and guidance within this policy to ‘Employees’ is also applicable to any of the Council’s contractors.

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

The Information Assurance Officer 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.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Human Resources.

8 Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of Customer and ICT Services
Accountable	Executive Director (Resources and Support Services)
Consulted	Information Security Group Executive Management Team Heads of Service Employees Consultative Cabinet Union
Informed	All Council Employees, All Councillors, relevant contractual third parties, partners and agents

9 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Audit Manager.

10 References

The following Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy;
- Internet Acceptable Usage Policy;
- Software Policy;
- GCSx Acceptable Usage Policy and Personal Commitment Statement;

- Computer, Telephone and Desk Use Policy;
- Remote Working Policy;
- Removable Media Policy;
- Information Retention / Disposal Policies; and
- Legal Responsibilities Policy.

The following Council policy documents are indirectly relevant to this policy:

- IT Access Policy;
- Human Resources Information Security Standards;
- Information Security Incident Management Policy;
- Communications and Operation Management Policy; and
- IT Infrastructure Policy.

11 Key Messages

- Members and employees should remember 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;
- 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;
- Data received should not be used for any purpose other than specified; and
- The Information Assurance Officer must always be notified of any new instances whereby data is to be transferred outside the organisation.

Appendix A

Electronic Data Transfer 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 transmitted externally that is protectively marked as PROTECT, RESTRICTED, CONFIDENTIAL , SECRET or TOP SECRET, as per the Council's adopted Government Protective Marking Scheme, must be subject to encryption, password protection and be at least compliant with current Information Security Policies. For further information on passwords to ensure adequate security, the Removable Media policy should be consulted. Should any employee require file encryption and password protection Customer and 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 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 is to be sent to external parties as this shall ensure the data is not 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 Assurance Officer is aware of the transfer (notification by Data Transfer Log, Appendix D); and
- Assurances that the recipient will handle the data in accordance with our security guidelines have been received. The Data Transfer Log (Appendix D) 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 Information Security 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 externally. In order to transmit this form of data, a GCSx email account shall be required. Please contact the Customer and ICT Services if you require assistance in transmitting sensitive information.

Where it is not possible to use a GCSx email account, contact with Customer and ICT Services should be made, who will be able to provide a suitable encryption method, i.e WinZip or Secure File Transfer Protocol (SFTP).

In addition, when sending information / data via email:

- Always use the Council email disclaimer, this is automatically added to outgoing email (if in doubt contact Customer and ICT Services 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 D); and
- Follow up any none-response within one 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.

Refer to the Council's Email Policy or contact Customer and ICT Services 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 Information Security Policies;
- Follow guidance in the sections below relating to Removable media / Removable Media policy;
- 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;
- **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 Customer and ICT Services can offer advice and support in relation this**;
- Ask the recipient to confirm receipt and record this on the data transfer log (Appendix D)
- Follow up any no response within one working day.

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

When Transferring data via an encrypted memory stick - all information covered by this policy must be subject to encryption, password protection and be at least compliant with current Information Security 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 Customer and ICT Services. 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.
In addition:

- Memory sticks from other organisations should be checked by Customer and ICT Services 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 Council network areas apart from where authorised by Customer and ICT Services;
- 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 Customer and ICT Services for advice; and
- 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 one 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 Information Security 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. Additionally:

- 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 Customer and ICT Services 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; and
- Virus and malware checking software must be used when the disk is placed in a Council machine.

For Further information please refer to the Information Security Policies.

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. For example, it is not possible to guarantee that the intended recipient has actually received the information.

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 its security be at least compliant with current Information Security Policies. Customer and ICT Services 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); and
- Ensure that you record your name, date and the time of the disclosure, the reason for it and who authorised it. Also record the recipient's name, and where appropriate; job title, organisation and telephone number. Use the data transfer log to assist (Appendix D).

Transfer of Data Held in Manual Form

For all personal information / data that is held in manual form, i.e. data held on hard-copy / paper based / non electronic format that is to be sent out externally the following must be undertaken:

- Confirm the name, department and address of the recipient;
- Seal the information in a robust envelope;
- Add details of the sender and data content;
- Mark the envelope 'Private and Confidential – to be opened by Addressee Only';
- When not transporting the data personally, trusted Couriers should be used particularly for large amounts of information. A list of approved couriers can be obtained from Support Services;
- In cases where just one or two sheets of information are to be sent about one or two data subjects, recorded or special delivery can be considered. As usual please contact the Information Asset Owner (the relevant Head of Service) before sending the information;
- Post should not usually be used as a method for transferring sensitive or personal data;
- Ask the recipient to confirm receipt and record this on the data transfer log (Appendix D); and
- Follow up any no response within one working day.

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 Audit Manager 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 who 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 Customer and ICT Services 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; and
- Inform the Information Assurance Officer via the Data Transfer Log (Appendix E).

Upon receiving data, a 'Data Transfer Log – Incoming Data' form must be completed and forwarded to the Information Assurance Officer (Appendix E).

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 Council 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 Head of Service / Business Manager.

The procedure should include at a minimum, all of the elements contained in either:

- for **outgoing** data;
  Appendix D;
  'Departmental Personal Data Transfer Procedures – Outgoing Personal Data'

Or

- for **incoming** data;
  Appendix E;

'Departmental Personal Data Transfer Procedures – Incoming Personal 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 Assurance Officer / Audit Manager immediately. If the Information Assurance Officer / Audit Manager are not available the Council's Head of Customer and ICT Services 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 Customer and ICT Services and Internal 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 Assurance Officer will notify:
   - The relevant Executive Director and Head of Service from who's remit the loss or potential loss originated;
   - The Data Protection Officer;
   - The Head of Customer and ICT Services; and
   - The Audit Manager.

2) The Information Assurance Officer 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 relevant Line Manager / Information Assurance Officer will, if necessary:-
   - Notify the individual concerned;
   - Advise the individual of their rights;
   - Provide the individual with appropriate support; and
   - Complete a Police incident report.

If the Information Assurance Officer is not available, the Audit 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 to a secure folder (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 C 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 C.

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

Corporate Standard for External data transfer

The corporate standard for external data transfer can be found in Appendix B.

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.

The Information Assurance Officer 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 Assurance Officer including systems in the testing phase.

For additional guidance on this matter please contact Customer and ICT Services.

Appendix B
Corporate Standard for External Data Transfer

This entire Data Transfer Policy and Procedure 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 Assurance Officer 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 of the receipt on the Outgoing data transfer Log (Appendix D);
- 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 Newcastle-under-Lyme Borough Council and any recipient of personal or sensitive data. An example of such a contract / agreement can be found in Appendix C;
- 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 Information Security and ICT Policies. (Customer and ICT Services 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 Assurance Officer 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 Customer and ICT Services 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 Information Security and ICT Policies. Management approval must be obtained;
- 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 Information Security and 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 Audit Manager / the Information Assurance Officer, Customer and ICT Services, the Insurance Section and the appropriate authorities (e.g. British transport police, local police, hotel security, etc.)

Appendix C
Example Data Sharing Agreement

All instances of data sharing whereby the Council intends 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 Newcastle-under-Lyme Borough 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 Information Security and 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 Newcastle-under-Lyme Borough Council to determine the appropriate retention period for all / any data transferred. After this time the data will be securely destroyed by the recipient, who will then inform Newcastle-under-Lyme Borough Council that this has been carried out.

Signed (Council) _____

Date _____

Signed (Third Party) _____

Date _____

Appendix D
Data Transfer Log – Outgoing Personal Data

To be used in instances of Personal Data Transfer **from Newcastle-under-Lyme Borough Council to an external destination**. No files are to be sent off site unless it can meet all of the following criteria:

- Abide by Newcastle-under-Lyme Borough Council Information Security and ICT Policies;
- 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 Audit Manager on ext. 2122 or Information Security Officer on ext. 2691.

Fully complete the following log, and once completed forward to the Information 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 (Signed, Head of Service):	Print Name: Date: / / Signed:
Receipt received from recipient	Date: / / Format : (e.g. email acknowledgement)
Signed (Audit Manager or Information Assurance Officer):	Signed: Date: / /

Appendix E
Data Transfer Log – Incoming Personal Data

To be used in instances of Data Transfer **from an external Source to Newcastle-under-Lyme Borough 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 Security Officer and/or Audit Manager; and
- Abide by the Council's Information Security and ICT Policies and the Data Protection Act.

If you have any queries regarding Data Security, please contact the Audit Manager on ext. 2122 or Information Security Officer on ext. 2691.

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

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 (Signed, Head of Service):	Print Name: Date: / / Signed:
Receipt sent to sender	Date: / / Format : (e.g. email acknowledgement)
Signed (Audit Manager or Information Security Officer):	Signed: Date: / /