DATA PROTECTION POLICY

1.0 Introduction

This document sets out West Lancashire Borough Council's policy regarding data protection. The Data Protection Act 1998 and the EC Data Protection Directive form the background to the document. The Policy is drafted using the terms of the Data Protection Act 1998. The Freedom of Information Act affects the Council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 enhances the protection and individual rights give under the Data Protection legislation.

The purpose of the data protection legislation is to regulate the way that personal information about individuals, whether held on computer, in a manual filing system or otherwise, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them and to require modification of the data if it is wrong and, in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The 1998 Act requires all processing of personal data to be notified to the Data Protection Commissioner and to be kept and used in accordance with the provisions of the Act.

2.0 Definitions

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are used:-

2.1 Data is information that is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose e.g. payroll system
- recorded with the intention that it should be processed by means of such equipment (CD ROM)
- recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system.
- one of a number of records to which public access is allowed e.g. information held by the Council (as a Housing Authority) for the purpose of its tenancies.

2.2 Data Controller means the Council as the organisation who determines how data is processed and for what purpose.

2.3 **Data Processor** means any person, other than an employee of the Council, who processes data on behalf of the data controller, e.g. someone contracted to the Council to deal with documents containing personal data.

2.4 **Data subject** is the individual about whom personal data is held.

2.5 **Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

2.6 **Sensitive Personal Data** means personal data consisting of information as to:-

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings

2.7 **Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:-

- organisation, adaptation or alteration
- retrieval, consultation or use of,
- dissemination, disclosure or otherwise making available
- combination, blocking, erasure or destruction of the information or data

2.8 **Relevant Filing System** means any information held manually in an organised structure either by reference to individuals or other criteria such that specific information about a particular individual is readily accessible.

2.9 **Special Purposes** means any one or more of the following ie journalistic, artistic or literary.

3.0 Principles

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing, and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are:-

1. Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless one of the conditions in Schedule 2 of the Act is met. These can be summarised as: where the individual has given consent; where the processing is necessary: for any contract, legal obligation, to protect the vital interests of the individual, or in the interests of justice and in the case of sensitive personal data at least one of the conditions in Schedule 3 of the Act is also met. The Schedule 3 conditions can be summarised as explicit consent, or where necessary for: employment obligations, vital interests, non-profit associations, manifestly made public, legal proceedings, administration of justice, medical purposes, ethnic monitoring

2. Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes

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

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

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

6. Personal data shall be processed in accordance with the rights of the data subject under this act (this includes the rights of subjects to access the data and to correct it)

7. Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security)

8 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.

These principles are regarded as the **minimum standards** of practice for any organisation with respect to personal data. Copies of the "Guidelines to the Data Protection Act", which illustrate these 8 principles are available from Sylvia Smith the Snr. Admin & Electoral Services Officer (extension 5031).

4.0 Policy

The Council Supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer, in manual files or otherwise and to increase the access given to individuals to information relating to them.

The Policy links to the other Council policies and documents for example:-

- ICT and Data Security Policy
- Retention and Disposal Schedule
- The Council's Constitution

- Code of Conduct
- Human Resources Policies
- Use of Internet & Email
- HIV and Aids Policy

It also links to the information sharing protocol with the Police Authority and to other initiatives under the Crime and Disorder Act 1998. There are a number of procedures underpinning this policy and guidance notes to supplement this policy for example:-

- Subject Access
- Registration/Notification
- New Systems
- Disclosures

To assist officers in complying with their Data Protection duties the Council has produced a collection of guidance notes, each relates to a specific area of data protection/security. These guidance notes are appended to this policy at Appendix 2

4.1 External and Internal Registration/Notification

The Council will have an external notification (registration) with the Information Commissioner which will be supplemented by an **internal register of sources and disclosures.**

4.2 Amount of data to be held

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected quickly.

4.3 Subject Access

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee of £10 will be charged for this service.

4.4 Public Registers

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals of these are examples set out in Appendix 1. Strict compliance with the legislation giving rights of access will be used in all cases.

4.5 Disclosures

Disclosures of information must be in accordance with the provisions of the Act, the Council's registration/notification and the internal register of sources and disclosures. The Council has a duty to disclose certain data to public authorities

such as the Inland Revenue, Customs and Excise and Benefits agency this will be done in accordance with the statutory and other requirements.

Disclosure within the authority either to Council officers or elected members will be on the basis of a need to know this will be judged when a request for information is made. The minimum of personal data will be made generally available.

4.6 System Design

The Council intends that personal data must be treated as confidential. Computer and other systems will be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users.

4.7 Training

It is the aim of the Council that all appropriate staff will be properly trained, fully informed of their obligations under the Act and aware of their personal liabilities.

4.8 Disciplinary Action

The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

5.0 Responsibilities

Overall responsibility for the efficient administration of the Data Protection legislation lies with the **Council** and is exercised by the Cabinet.

5.1 Managing Directors and Heads of Service

Day to day responsibility for administration and compliance with the act is delegated to the Managing Directors and Heads of Service, for compliance with the Act's provisions within their respective areas of authority. Within each Service, Data Protection Link Officers may be appointed to undertake administration of data protection and to assist in compliance with the requirements of the legislation on behalf of the Managing Directors and Heads of Service (the number of Data Protection Link Officers in each Service will be a matter for the Heads of Service to determine).

5.2 Data Protection Officer (Snr. Admin & Electoral Services Officer)

It is the responsibility of the Data Protection Officer to assist the Council to ensure compliance with this policy, to specify the procedures to be adopted and to co-ordinate the activities of the designated Link Officers.

The main duties of the Data Protection Officer are:-

- maintenance of the Council's external registration/notification under the Act, and to act as liaison officer with the Information Commissioner

- development, updating and publication of data protection procedures for the Council.

- maintenance of the internal register of sources and disclosures and in association with the internal Audit Section to audit data protection procedures and practices.

- initial contact point for subject access requests.

- in conjunction with Human Resources, provision of education and training seminars regarding data protection issues

5.3 Senior Information Risk Owner (SIRO)

The Borough Solicitor acts as the Council's SIRO. The SIRO

- is the officer who is ultimately accountable for the assurance of information security at the Council
- champions information security at Directorate Service Head (DSH) level
- owns the corporate information security policy
- provides an annual statement of the security of information assets for the Annual Governance Statement (as part of the audit process)
- receives strategic information risk management training at least once a year

5.4 Information Governance/Data Protection Working Group (the Group)

This group, chaired by the SIRO, is comprised of representatives from Legal and Democracy, Finance, ICT, Internal Audit, Risk Management and the Data Protection Officer. Representatives of other sections attend meetings as required. The Group develops policy and guidance on information security and maintains a reporting procedure for information security breaches. The Group supports the SIRO and its remit is to:

- review and develop the Council's information security strategy.
- review and develop information security policies and guidance and ratify changes to these, including ongoing review of relevant Council Policies, e.g. Data Protection Policy and ICT and Data Security Policy and Retention and Disposal Policy.
- co-ordinate a data protection review within Services, to include: compliance, cataloguing of data resources, training requirements, document assessment, e.g. for privacy notice/customer notification.
- assist in a coordinated approach to Service Specific Data Protection Procedures
- assist with management of security risks in projects through the project life cycle
- review all reported security breaches and report them regularly (and immediately where appropriate) to the SIRO and onward to Government Connect where appropriate

- as appropriate, report information security breaches to the Information Commissioner via the SIRO
- promote awareness of information security by all officers and Members
- plan, develop and deliver training on information security in consultation with the Transformation Manager.

5.5 Information Asset Owners (IAO)

IAOs are senior managers/software system supervisors across the Council who are currently responsible for the main information systems and information assets. In terms of information security their responsibilities are:

- to manage security, compliance and risks associated with their information assets
- to carry out an annual assessment of information risk as part of risk management
- to ensure that staff accessing the systems are made aware of security issues and acceptable use and receive training as necessary
- to ensure that information security incidents are reported via the Council's information security incident reporting procedure
- to ensure that actions are taken to remedy breaches
- to classify information assets in line with corporate policies. Using a classification scheme for sensitive and confidential information.
- to receive information risk management training annually
- to consider on an annual basis how better use could be made of their information assets within the law

5.6 Data Protection Link Officers

The Data Protection Link Officers are responsible to the Managing Directors and Heads of Service for:-

- liaison with the Data Protection Officer on all matters concerning administration of the Act
- working with the Managing Directors and Heads of Service to ensure compliance with the notification (registration) particulars in respect of systems within the Service;
- working with the Service Managers and the SIRO to ensure awareness of the Act within the Service, and to ensure that the control and handling of personal data within the Division does not contravene the Data Protection Principles or Council procedures.
- assisting the Data Protection Officer in the collation and validation of external and internal registration particulars relevant to the Service, and advising the Data Protection Officer of any planned changes to the registration particulars
- assisting in the response to access requests from data subjects.

5.7 Officers and Members

In addition to the formal responsibilities outlined above, all officers and members have a duty to observe the Principles of the Act and the procedures referred to in this document.

Individuals who do not handle personal data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

Disciplinary action may result if the Data Protection Principles or procedures outlined in this document are breached.

(Ref DATA PROTECTION POLICY 17th January 2013)

Appendix 1

Examples of Publicly available information that could be used to identify individuals

Elections
Representation of the Peoples Act 2000
Register of persons who are eligible to vote in elections

Returns or declarations and accompanying documents relating to election expenses sent by a candidate of a parliamentary or local government election to the Council

Disclosable Pecuniary Interests
Local Government Act 2011 - The Relevant Authorities (Disclosable Pecuniary Interests) Regulations 2012.

A register setting out certain information which elected members give on their interests

Members Allowances
The Local Authority (Members' Allowances) Regulations 1991 as amended by The Local Authority (Members' Allowances)(Amendment) Act Regulations 2003

Records of payments made to elected members are open to inspection by local government electors for the area. Additionally, the authority must publish within its own area details of the total sums paid under the scheme.

Committee Minutes Reports etc
Local Government Act 1972

Allows access to agendas and reports of committees and subcommittees. Minutes are also available

Taxis and Private Hire Vehicles
Town Police Clauses Act 1847
Local Government (Miscellaneous Provisions) Act 1976

Register containing information about owners and drivers of taxis and drivers of private hire vehicles.

APPENDIX 2

DATA PROTECTION GUIDANCE NOTES

1. Checking entitlement procedure
2. Email procedure
3. Fax procedure
4. Phone procedure
5. Office security procedure
6. Paper records out of the office procedure
7. Clear desk procedure
8. Checklist for privacy notices on applications and other forms.
9. Procedure for sending personal information in the post
10. Contractor checklist
11. Checklist for data sharing agreement or protocol
12. Building & Network Security Procedure
13. Information Security Incident Management Procedure
14. GCSx Acceptable Usage Policy

WLBC DP GUIDANCE NOTE 1

Checking entitlement procedure

Whenever you receive a request to transfer personal, sensitive or confidential data, the first step to take is to ensure that the person who has asked for the information is who they say they are, and is entitled to receive the information.

Before disclosing any personal, sensitive or confidential information, you should be sure that you know

- Who is asking
- What information they want
- Why they need to know
- Whether they have a legal power to demand the information
- Whether the Council has already agreed to supply the information
- If neither of the above two apply, whether you have the consent of the subject or owner of the information to supply it

With any organisation with whom you have regular, routine contact, you should agree a specific way of asking for information and specific officers who are entitled to ask. This can speed up responses to legitimate requests considerably.

Requests received by phone

- No matter who the caller is, if you are in any doubt about whether the request is valid, ask the caller to put their request in writing

- If the requester is a customer or other member of the public, ask them two questions that only they are likely to know the answer to – a reference number relevant to their service, when their service started, or similar

- If the requester is a family member or friend of a service user or staff member, do not provide information unless you have the person's consent (either previously obtained in writing, or from the person themselves if they are also present on the call). If consent has not been provided, ask for the request to be put in writing, or for the service user to get in touch first

- If the requester is from the police or another official body, ask them to put their request in writing. If they say that the request is an emergency, ask for their name, who they represent, and what data they need and why they need it. If the request is valid, call them back via their switchboard or main contact number, not a direct dial number. Check this on the organisation's website.

Requests received by email

An email address that ends in gov.uk, @police.pnn.uk, @nhs.net, or gscx.gov.uk or gsi.gov.uk is very likely to be valid. An email received from such an address is likely to be genuine, but this does not remove the requirement to check entitlement.

WLBC DP GUIDANCE NOTE 2

Email procedure

1 General advice

All staff, volunteers and contractors need to keep personal information about individuals secure and private at all times. Email is convenient and fast but it carries a series of risks:

- It is very easy to send information to the wrong people
- Data in an email is very portable, and can easily be forwarded to others

Never send an email when annoyed or frustrated. The language and tone of an email should be appropriate for context – an email can have the same legal status as a signed letter on headed paper. Assume that this might happen to your email and write it accordingly. Keep work and personal issues separate. Remember that any personal data may be requested by the person about whom it is recorded.

If sending sensitive or potentially damaging information in an email – stop and think. Is email the best and most secure way to circulate the information?

2 Requirements

- When sending sensitive information (e.g. information about criminal activity, health or other potentially damaging information), use encrypted email where available

- If password-protecting an attached document, do not send the password by email – contact the recipients separately to provide the password, and change it every time. Be aware that dictionary words are not a secure password

- Check that you have used the right email address

- Never let the email software fill in a person's email – type in the whole address, or choose it from an address book. If you have previously emailed a person with a similar name to your recipient, the software might fill in the wrong address

- If copying people into an email, always use the BCC ('blind copy') function unless you are certain that each recipient already knows the other's address. If sending emails to home addresses, use BCC automatically.

- If using an email distribution list, check before sending the email that you have selected the correct one and the only the right people will receive whatever you are sending

- Check that you have added the right attachment before sending an email

- If forwarding information, include only the parts of the email you want the recipient to see. Never forward a long email chain unless you are certain that the recipient is entitled to all of the information in the chain. Look at where the conversation started, and what else is included

WLBC DP GUIDANCE NOTE 3

Fax/Photocopier/Scanner procedure

A. Use of Fax

1. General principles

Fax machines are not a secure method of transmitting information and should only be used if no other method is available. For both confidentiality and legal reasons, it is vital that care is taken when sending a fax. Faxing information carries a number of risks:

- It is easy to fax information to the wrong place by dialling the wrong number or using one which is out of date, and you cannot recall a fax easily
- The quality of copies on arrival cannot be guaranteed - this can lead to inaccuracies and misreading of information
- You do not know who is on the other end of a fax machine, and who might see it when it arrives

2 Procedure for faxing

For staff, volunteers and contractors

When sending a fax containing confidential or personal information, you must always follow this procedure:

- Ask yourself: should I send this as a fax, or is there a safer alternative?

- **Always use a cover sheet** marked 'Private and Confidential' and which contains:

    - A named recipient, or at least a team name

    - Your name, job title, team, location, your telephone number and fax number

    - The number of pages you are sending, including the cover sheet

    - an explanation of what to do if the fax has been received by the wrong person (e.g. contact you immediately, and do not read or share the contents with anyone else)

- Before you send a fax containing personal or other sensitive data, **telephone the intended recipient** to let them know you are sending a confidential fax and agree a fax number.

- Keep any transaction reports or receipts as evidence of where the fax was sent in case it was sent to the wrong person, so you have a chance of contacting the recipient

- **Ask the recipient to ring you back to confirm receipt**, or ring them yourself after you have sent the fax

- Ensure they confirm that all pages have been received

- **If using a pre-programmed fax number, ensure that you choose the right one**, and regularly check that the pre-programmed numbers are still correct

- If you are entering the number manually, **double-check it** to make sure you are using the right number

For Managers

- You must be aware of what your staff are using fax machines for, who they are sending them to, and why fax is being used as an alternative to other methods. Consider whether fax remains the right way to share information – secure email may be an alternative

- Your fax machine should be in a restricted location, not in a public area of your building where faxes can be picked up by anyone who is not part of your team or not authorised to see the information that is being received. If staff pick up your faxes from a central location, they must be instructed not to read faxes, and to bring them straight to your team. You should consider whether this arrangement is secure.

- You should ensure that a member of your team regularly checks any pre-programmed fax numbers to ensure that they remain correct and up-to-date

B. Photocopying, Printing and Scanning

You must ensure that you take all copies of information from the machine once you have finished copying and do not leave any personal information at the copier.

If you send information to a printer used by other members of staff you must always collect your printing straight away and not leave it on the printer allowing other people to see/take the information.

If you are scanning any information, you must ensure that you send it to the correct recipient. As with email, if you are using a recipient distribution list then you must check before you send the scanned information that you have selected the correct recipient and that only the right people will receive whatever you are sending.

WLBC DP GUIDANCE NOTE 4

Phone procedure

1 General principles

For both confidentiality and legal reasons, it is vital that care is taken when providing or receiving information over the phone. Sharing information over the phone carries a number of risks:

- Information may be transcribed incorrectly
- You cannot always be certain who you are speaking to
- You can be overheard

2 When a member of the public calls you

- Ask at least two security questions, appropriate to the service you work in for example a reference number for the service and when their service started. Tell the caller you are asking these questions to make sure that you are dealing with the right person – **do not mention Data Protection.**
- If they are asking about someone else's case or problem, do not provide personal information unless you have the person's consent (either previously obtained in writing or from the person themselves if they are also present on the call). If consent has not been provided, politely explain that you need consent to continue, ask for the request to be put in writing or for the service user to get in touch first to authorise you speak to a nominated person on their behalf.

3 When someone from another organisation calls you asking for information

- Identify the person clearly, check who they work for and what they want
- If they demand information, check their entitlement to demand it – ask what law or right allows them to demand the information
- Unless you are certain that the person is who they say they are, get their switchboard number (not their direct number) and ring them back. Check the switchboard number from their website, not from them
- If in doubt, ask them to put the request in writing

4 When you call someone

- If calling to provide information, be certain that the phone is the best way to provide information – would a fax or email be better (both allow a specific record of the information to be provided)?

- Ensure you speak to the person who needs the information – do not leave personal or sensitive data in a message

5 When someone calls to provide you with information

- Ensure you record information accurately – check the information with the person providing it. Do you have the spelling, numbers and details right?

Remember: Security questions are only necessary when you are being asked to disclose personal information.

WLBC DP GUIDANCE NOTE 5

Office security procedure

1 Introduction

Trustworthy and trusted staff are the best defence against internal and external security threats, but they must be supported by sensible procedures.

Managers must take all reasonable steps to ensure that information is secure. You should remember that you are protecting personal information as much from accidental disclosure as deliberate theft**.**

Managers must ensure the following:

- The workplace is secure, and the risks have been properly assessed
- All staff have received Data Protection and confidentiality training
- All staff have read and understood policies on Data Protection, information security, appropriate IT usage, and information sharing

2 General office checklist

- Are paper files containing personal data locked away when not in use?
- In areas accessible to the public, have you ensured that there is no personal data on display (i.e. on whiteboards or noticeboards)?
- In open-plan offices, are there secure areas for confidential discussions and phone calls?
- Are offices where personal data is stored or on display used as thoroughfares to other parts of the building? If so, are measures in place to protect the data from being seen?
- Are computer screens not visible in areas to which the public have access, and are they angled away from windows?
- Do you ensure that passwords or login information are not written down, or recorded anywhere? Do not allow anyone else to use your password.
- Change your password regularly and immediately if you think someone else has identified it.
- Are PCs and laptops set up to log out when not in use?
- Do managers authorise the removal of paper files from the office?
- Is there a system in place to log the removal of paper files from where they are stored (either a file removal form left in where they are stored, or an electronic record)? This should show who has a file, and if it is removed from the office, where it is being taken to.
- Confidential files should be password protected if there is a risk of them being accessed by unauthorised staff.
- Is there an effective back up system in place and is data stored on a shared sever file where possible?

- Passwords should only be used by the authorised owner. Enhanced password controls on the Authority's network include the following restrictions:
- Minimum of 7 characters
- Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Must contain characters from three of the following categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphabetic characters (e.g. !, $, £, %)
- Must be changed a minimum of every 90 days
- Must not be used within 20 password changes

- Forgotten passwords can only be reset by contacting the ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk

3 Visitors

Office areas should be open and welcoming, but security measures must be in place. Offices that do not have access controls need different forms of security to places where access is controlled.

- All areas where sensitive information is used or stored should introduce access controls where they are not already in place
- Contractors should sign, or have in place, a confidentiality agreement when entering the premises.
- All visitors should be obliged to sign-in, wear an ID badge and should generally be accompanied when on site.
- If a contractor or visitor requires either a door access swipe and/or network login submit their details to Admin & Elections and ensure that the door access swipe is retrieved before the contract/visitor leaves the site and, if they have been provided with a network login, that the ICT Service Desk is informed to ensure network access is disabled.

- Anyone not displaying an ID badge should be challenged, asked who they are and where they are going

4 End of the day

- Paperwork should be cleared from desk
- All filing cabinets and drawers should be locked
- Portable electronic equipment – laptops, memory sticks, mobile phones – should be out of sight and locked away
- All windows should be closed and locked
- Curtains and blinds should be drawn to deter opportunist thieves

5 Physical disposal of information

If information is not shredded within the office, confidential waste bins must be available. These should be sealed – confidential waste bags should only be used as a short-term measure. Bags of confidential waste must never be left out for any period of time. All shredding must be undertaken in accordance with the Council's Retention and Disposal Schedule and a record of files destroyed must be maintained.

6. Staff leaving the Council

When staff leave the employment of the authority, it is the responsibility of their line manager to notify the ICT Services to enable their network logon to be disabled and to remove the ID and password from the system that the member of staff used. In addition, Admin and Elections should be informed so that the door access is disabled.

7. File review

All files (including physical and electronic files and/or records) should be reviewed periodically. Reviews should take place at least once a year and, more frequently if circumstances require, to ensure the obligations set out are followed. Current working files should be continually monitored and therefore should always be compliant with the requirements of the Act. All officers are responsible for ensuring that their files comply. Closed files should be reviewed in accordance with a programme for review agreed with the Link Officer (most probably dictated by the type of personal data held and the subject area of the file).

Manager see also the Building Security Procedure

WLBC DP GUIDANCE NOTE (6)

Records out of the office procedure

1 Introduction

Staff who need to use paper records containing personal or other confidential data out of the office should ensure that the records must be safe at all times. An encrypted laptop or other form of remote, secure access to information may be a safer alternative and should always be considered. Managers should be aware that their staff are removing files from the office, and ensure that this procedure is followed.

2 Basic principles

- Managers should approve the circumstances in which paper records are removed from the office, and by whom

- The removal of a file from the office should be logged – the log must identify where the record has been taken, when, why and by whom.

- Records should be removed only where necessary, and only for the minimum time required. They should be returned as soon as possible.

3 Records out of the office

- Staff carrying paper documents are responsible for their safety – even if they are carrying documents for someone else.

- Files or folders should only be removed if in a safe and transportable state. There must be no loose papers. A file that is damaged or too large should be re-filed and restored before being taken out

- Files or documents should always be carried in a bag when out of the office. Paper records should not be carried loose. Even if documents are held in a robust file, that file should be carried in a lockable, waterproof bag. An open shopping or carrier bag is never an appropriate way to carry personal data, or confidential or sensitive documents

- Where records are routinely removed from the office as part of the normal course of work, a lockable case or bag should be available at the office

- Where larger quantities of records are routinely removed from the office, a lockable wheeled case should be available at the office

- Under no circumstances should staff read files or records containing personal data on public transport, in restaurants or cafes, or anywhere else where they can be overlooked

- Never leave documents, files or folders unattended, or on show in a car or other vehicle. Always lock them in the boot.

- Before leaving any building, car or public transport, and before you drive away from any location where you have been using paper records, staff should make a conscious check that they have everything with them.

- Paper records should only be in transit during the working day – staff must not carry paper records to pubs, restaurants or other social venues

4. Records at home

- Never leave paper records in your car overnight. If you need to return home with documents containing personal or sensitive data, take them into your home and keep them safe. Ensure that family members do not read or access them.

- If you leave records at home for any reason when you are not there, they should be stored out of sight in a cupboard or drawer.

- Do not store paper records with laptops or other valuables.

5. Use of Portable Computers, PDAs and Mobile Phones for Remote and Homeworking

- Mobile devices, hard copy documents and files should only be removed from the office when that removal has been appropriately authorised. When laptop computers are being transported a carrying case should preferably be used to reduce the risk of accidental damage.

- Computer equipment must not be left unattended in a vehicle unless all doors, windows and other means of access have been secured and locked and all keys of the vehicle removed to a place of safety, and the equipment placed in the boot of the vehicle. The insurers accept that the rear compartment of a hatchback vehicle is considered to be the boot as long as the equipment is stored under the factory fitted cover. Failure to adhere to this will mean that insurance cover will not be available. In the case of overnight storage this should be in a secure building e.g. an officer's house.

- Laptops, memory sticks and removable disks should be encrypted and/or password protected when taken out of the office. Mobile phones and other palm top devices e.g. PDAs should also be password protected. For guidance contact the ICT Service Desk on 0845 053 0042 or email: ICTServicedesk@oneconnectlimited.co.uk.

- All reasonable precautions must be taken to prevent or minimise accident, injury, loss or damage.

- The users of portable computers in a public place should be vigilant as theft is common. Sensitive information should not be displayed in a public place where it could be overlooked.

- No sensitive information should be held on the computer hard drive. Sensitive information should not be transported outside the United Kingdom.

- Only those with legitimate or approved access must use the computer equipment.

- Only software authorised by the Authority must be used. Security backups of data should be taken on a regular basis.

- If any computer equipment, PDA or mobile phone is lost or stolen then this should be reported to the ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk.

WLBC DP GUIDANCE NOTE (7)

Clear Desk Procedure

1 General principles

The purpose of a clear desk procedure is to limit the risk of paper records being lost, stolen, inappropriately accessed or damaged by contractors and visitors, staff not directly involved in providing services to the individual, or even thieves and vandals. The principle for handling records should be as follows: **information of any kind should be accessible only to those who need it, and only when they are using it.**

2 Practical measures

2.1 Paper records

- Desks must be cleared of any confidential or person identifiable information when you leave the office for the day

- Where available, paper should be stored in locked cabinets or other secure furniture when not in use. Where secure storage is not available but is deemed appropriate, this should be raised with managers.

- Where lockable furniture is not available, the doors to the office must be locked by the last person to leave

- Confidential or personal information, when printed, should be removed from printers or faxes immediately

- Paper records which are no longer required must be stored securely for disposal, which should happen as soon as possible

- In a public area, or an area to which the public or visitors have routine access, no paper files or records should be left out unless the visitor is supervised at all times

- Keys used to lock away records should not be left on display, and should be locked in a key cabinet where available. The codes for doors or locks must never be on display.

- Visitor, appointment or message books should be locked away when not in use.

2.2 Computer records

- Passwords must not be written down and you should not tell anyone (or allow someone else to use) your password. Users should change their passwords regularly and immediately if they believe someone else has

identified it. Personal data must only be held on a PC which is password protected and/or encrypted to prevent authorised access.

- Screens must be locked when computers are left unattended, irrespective of the amount of time spent away

- Screen locks should be used, so that a computer locks itself if left unattended

- Computer screens should be positioned away from the view of visitors or the public, and angled away from windows

- Where it is not possible to position screens out of sight, they should be closed, minimised or locked when unauthorised persons are in close proximity

Consideration should be given to the use of staff's personal mobile phones/cameras in the office and whether this is a security concern

WLBC DP GUIDANCE NOTE (8)

Checklist for privacy notices on application and other forms

The purpose of a privacy notice is straightforward: it tells the person whose information is being gathered what you intend to do with their information and who you will share it with or disclose it to. There is a fundamental difference between telling someone how you are going to use their personal information and getting their consent for it so it is important to be certain about which one you are doing.

The collection and use of personal information is often essential to provide the service the individual has requested and/or may be required by law and therefore choice is not an issue.

If you are telling the person what happens to their data, this is a privacy notice. The privacy notice should be a clear description of what you are going to do, using a simple to understand heading i.e. 'How we use your information".

If you are asking the person for permission to use their data, then the privacy notice should come first, and then you should ask for consent in a clear and unambiguous way. Bear in mind that if you are asking for consent, if the person refuses, you should respect that. You can, nevertheless, point out what will happen if they do refuse.

If the use of data is complicated, give the person the main points on your form, and then tell them where they can find more detail (for example you can have a layered privacy notice with the main headlines on an application form, and then a website page or a separate leaflet).

- Before you start, has the amount of information being requested been measured against the purpose for which it is being gathered? Is anything being asked for that is not really needed, and is there any data that is required that is not asked for on the form?

- Is the form in plain English, making clear what the person is being asked for, and why the information is being gathered?

- Could any of the information gathered be taken anonymously, and still achieve the same objective?

- Have you provided enough options to allow people to give full and accurate answers?

- Is any check or verification carried out on the information (i.e. taking up references, credit check)? If so, is this made clear?

- Is any of the information collected shared with another organisation like the council, voluntary organisation or health bodies? If so, have you made this clear and told them who you will share it with?

- Is the information that you are collecting used for any purpose not stated on the form? For example, is feedback or complaints data being used to make decisions about services provided to a resident? If so, this must be explained clearly on the form or as part of the process.

- Is the person whose data is being collected likely to be surprised by how their data is being used? If so, what can you do to prevent that?

- Are the replies to questions mandatory or voluntary?

- Does the notice explain the consequences of not providing the information? For example non receipt of a benefit

- Does it explain what you are doing to ensure the security of their personal information?

- Does it explain their rights and how they can exercise them? For example the fact that they can obtain a copy of their personal information or object to direct marketing

- Does it explain who to contact if they want to complain or know more about how their information is being used?

- **Remember to review your privacy notices regularly**

Examples of clauses to be used in a privacy notice: These would need to be tailored to each service:

How information about you will be used.

We collect personal information when you register with us to request a service, when you voluntarily complete customer surveys and provide feedback.

We collect information about you to provide you with a required service and to manage your account.

We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, as well as those of selected third parties, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

□ Post □ Phone □ Email □ SMS

We would also like to share your information with other companies so that they may send you information about their products and services, by post, telephone, email and SMS. If you agree to your information being shared in this way, please tick the box □

You have the right to request a copy of the information that we hold about you. If you need any further information on how your information is being used, if you require a copy of the information we hold or if you wish to make a complaint then please contact…….

WLBC DP GUIDANCE NOTE (9)

Procedure for sending personal information in the post

1 Introduction

When sending out paper documents containing personal data, you must ensure that documents are secure and properly addressed. You should bear in mind that some methods of post are more secure than others. The more sensitive the information being sent, the more secure the method of transmission required.

The person sending the document is responsible for ensuring that they are sent to the right people, safely packaged, and that they can safely be returned if not successfully delivered.

Some of the risks involved in posting out records include:

- Using a previously written letter or document as a template but leaving addresses or other inaccurate data in the new document
- Sending the wrong documents out, or using the wrong address

2 For staff, volunteers and contractors

YOU MUST:

- Send only documents that are required rather than whole files. Consider whether a copy of the document, rather than the original would suffice. The loss of a copy is a less serious incident than the loss of the original.

- Ensure that the destination you are sending documents to is still in the same place – especially if the recipient is outside the Council.

- Check the address to ensure that it is correct, and send documents to a named person if at all possible, and not to a department or team.

- Check **everything** that you put into the envelope or package, no matter how much of a hurry you are in. Ensure that only the documents you intend to send are included.

- Always put either a covering letter or a compliment slip containing your contact details in the envelope with the information – DO NOT put records or data into an envelope by themselves

- Write your return address on the back of the envelope or package – this will allow a wrongly delivered envelope to be returned without having to be opened

- Seal the envelope securely and mark it Private and Confidential

- Send any personal or other sensitive information by recorded delivery, and keep the tracking information so you can find out when it was delivered

WLBC DP GUIDANCE NOTE (10)

Contractor checklist

A data processor may be a courier who you regularly use to transfer your records, an IT specialist coming in to work on your systems, a consultant or a contractor to whom you outsource work, projects or services. If they handle, analyse, cleanse, send out, shred or collect data for your purposes, you should ask these questions BEFORE you complete a contract. No matter how good a job your contractor does, if you do not get security protections in writing, you do not have them. They are not liable for security breaches – you are.

1 Have you got a written agreement or contract with your processor, which sets out what the job is, and how any personal data will be used?

2 Does it include guarantees that the contractor has adequate security in place to look after your data and require the contractor to act only on your instructions?

3 In general, are the security arrangements set out in the contract at least as strong as the security you have in place when using the data you intend to supply to them?

4 Have you specifically set out what security arrangements they should put in place? This will depend on the arrangement, but some examples include:

- Have you insisted that any laptops, pen drives or other portable media are encrypted?
- Have you required the contractor to put in place appropriate security when moving paper records around?
- Have you insisted on secure storage when personal data is held at their premises – does paperwork need to be locked away, is information stored on systems which have anti-virus protection, back-ups and firewalls

5 Have you set out what will happen to data when the project is completed – i.e. destroy data with confirmation or return all copies to you?

6 Have you set out restrictions on what the contractor can do with the data, whom they can share it with, and which of their staff is entitled to access and use the data? Make sure the organisation has appropriate security checks on their staff.

7 Have you confirmed that the contractor cannot use the data for their own purposes, and cannot disclose it to a third party without your express permission?

8 Have you put in place a mechanism to monitor the contractor's compliance with these arrangements?

9. Make sure the contract requires the contractor to report any security breaches or other problems to you and have procedures in place on how you will act if a problem is reported.

Below are some examples of a DPA clause for inclusion in contracts. These are examples only and in every case when you are engaging a contractor you will need to ensure that suitable clauses are in place to protect the Council. Please consult your manager and Legal Services if in any doubt.

The Council is the data controller for the purposes of the Data Protection Act 1998 and the Contractor hereby undertakes that any personal data provided under this Agreement shall be dealt with by him only in accordance with the instructions of the Council and at all times within the requirements of the Data Protection Act 1998 (as amended from time to time). Without prejudice to the generality of the foregoing the Contractor shall:

- have and maintain in place technical and organisational measures governing the processing of the Council's personal data in accordance with the requirements of the seventh data protection principle;
- take all reasonable steps to ensure the reliability of any employees who may have access to the Council's personal data;
- prevent disclosure of any personal data supplied by the Council other than to those members of staff who necessarily require that data for the purposes of carrying out the Contractors obligations under this Agreement.

The Contractor hereby agrees to supply to the Council upon request and within 10 days all information supplied or obtained in the carrying out the agreement as required from the Council in accordance with a request made to it under the Freedom of Information Act 2000.

Or

Data Protection

(a) Without prejudice to any other obligations herein the Contractor shall:

(i) comply with each of the provisions of the Data Protection Act 1998 ("the Act") as amended or replaced from time to time, together with any regulations or Codes of Practice for the time being in force in relation to the Contract Works as if it were a data controller including without limitation the data protection principles set out in Schedule 1 to the Act;

(ii) carry out all data processing in compliance with the requirements of the Act and all equivalent legislation in any other country. In particular, it will comply at all times with good industry practice which shall mean that it shall exercise the degree of skill, due diligence, prudence and foresight that would reasonably and ordinarily be expected from a skilled and experienced person engaged in the provision of personal data processing services;

(iii) only process personal data that it will be processing on the Council's behalf as instructed by the Council. The Contractor shall not carry out any other processing use or disclosure using such personal data.

(b) Security Measures – The Contractor shall:

(i) have in place and at all times maintain appropriate technical and organisational security measures governing the processing of the Council's personal data in accordance with the requirements of Schedule 1, Section 7 of the Act.

(ii) meet to discuss the processing the state of technological development and the best methods by which personal data may be kept secure, up-to-date, and assessed for relevance, accuracy and adequacy, and to plan for the implementation of any new security procedures relating to the processing of personal data.

(c) Employees – The Contractor:

(i) undertakes to take all reasonable steps to ensure the reliability and suitability of any employees who may have access to the Council's personal data.

(d) General – The Contractor shall:

(i) notify the Council immediately of any notice of non-compliance with or request for information under the Act (or any equivalent legislation in any other country) and co-operate fully and promptly and to provide to the Council all reasonable assistance in dealing with any such notice or request;

(ii) not under any circumstances transfer any of the personal data that it may process on the Council's behalf to any country or territory outside the European Economic Area without the Council's prior written consent which may be withheld in its absolute discretion;

(iii) on termination of this agreement for any reason, immediately cease all processing of the Council's personal data and will return to the Council in a format specified by the Council or destroy as the Council may request in its discretion all personal data processed by the Contractor on the Council's behalf

WLBC DP GUIDANCE NOTE (11)
Checklist for a data sharing agreement or protocol

Each question comes from the Information Commissioner's Code of Practice on Data Sharing – the answer to each question should be yes.

	Element of Code of Practice	**Yes**
1	Is the objective for sharing data set out in the protocol?	
2	Is the legal justification for sharing set out in the protocol?	
3	Are organisations signing up to the protocol included in the document?	
4	Is the data that needs to be shared required described in detail?	
5	Is the way data should be shared included, including nominated people or roles who need to send / receive data?	
6	When and how often will data be shared?	
7	Is there a mechanism for checking the effectiveness of the protocol?	
8	Have the risks of sharing been documented?	
9	Are security measures documented in the protocol	
10	Has the necessity of sharing been assessed?	
11	Have protocol signatories checked / amended their notifications?	
12	Will any data be transferred outside EEA and are processes related to this documented?	
13	Are DPA Principle 1 conditions properly addressed?	
14	Is DPA Principle 1 fairness properly addressed?	
15	Does the protocol include provision for data quality to be confirmed before sharing? • Accuracy • Agreed format for sharing data • Compatibility of systems • Retention / deletion of data • Correction of inaccurate data	
16	Does the protocol include procedures for subject access requests, complaints and queries from data subjects?	
17	Does the protocol include requirements for staff training?	
18	Does the protocol include sanctions for corporate failure to comply with the protocol?	
19	Does the protocol include procedures for dealing with breaches of security and other breaches of the Data Protection Act, duties of confidentiality and other legal obligations?	
20	Are breaches clearly defined?	
21	Does the protocol include a process to terminate the agreement?	
22	Does the protocol set out processes for reviewing the basic necessity of data sharing?	

WLBC DP GUIDANCE NOTE (12)

Building and Network Security Procedures

To ensure the security of corporate buildings and the authority's corporate network please can all managers adhere to the following procedure for door access swipe cards and/or network usernames for new starters, contractors, visitors and other third parties.

1. New Member of Staff (including Agency Staff)

When a new member of staff starts, it is the responsibility of the line manager to provide the Admin and Elections section with the following information.

- Name of new employee
- Section/Service
- Photograph (This can be e-mailed if you have access to a camera, otherwise please bring the member of staff to the Admin and Elections office to have their photo taken)
- Payroll Number
- Car Registration (if applicable)
- Whether the cards should be sent via internal mail or collected.

If access to the Council network is required, please e-mail the ICT Service Desk the following details:

- Name of new employee
- Section/Service
- Job Title
- Which systems the user will require access.

The login details will then be e-mailed back to you. When the user logs in for the first time they will then be asked to create a new unique password.

2. Staff Leaving

When a member of staff leaves it is the responsibility of the line manager to inform the Admin and Elections Section and the ICT Service Desk to ensure that their door access permission and ICT network username are deleted/disabled. Systems Administrators should be instructed by the line manager to remove the ID and password from the application software system that the member of staff used.

Please ensure that their door access swipe card is retrieved on the last day of employment.

3. Contractors/Temporary Passes

Any visitors accessing the back offices at 52 Derby Street must obtain a visitor badge from reception and wear this whilst on the premises. Officers organising meetings in the Council Chamber/Cabinet-committee room do not need a visitors badge but the officer organising the meeting will be responsible for their visitor(s) at all times. You must ensure that your visitor(s) returns their visitors badge at the end of the visit.

If a contractor or visitor requires either a door access swipe and/or a network logon, the line manager should provide Admin and Elections and/or the ICT Service Desk with the following relevant details:

- Name
- Company
- WLBC member of staff they are working for/visiting.
- Which system(s) they require access to.
- How long they plan to be onsite.

The line manager should ensure that the door access swipe card is retrieved before the contractor/visitor leaves the site and if they have been provided with a network logon that the ICT Service Desk is informed to ensure network access is disabled.

In addition to the above procedure and to further enhance building and network security, any swipe card or network login not used within a 2-month period will be disabled.

If you have any queries regarding this procedure, please contact either ICT Service Desk on 0845 053 0042 or email: ICT Servicedesk@oneconnectlimited.co.uk or Admin and Elections (EXT 5013).

WLBC DP Guidance note 13

Information Security Incident Management Procedure

If despite the security measures you take to protect the personal data you hold a security breach occurs, it is important that you deal with the breach appropriately.

Scope

This procedure applies to all Employees, Councillors, Agency Staff, Partners, and contractual third parties of the Council who use or have access to, or custody of WLBC personal data.

All users must understand and adopt this procedure and are responsible for ensuring the safety and security of the Council's personal data that they use or have access to.

A data security incident can happen for a number of reasons ie loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, equipment failure, human error, hacking attack, blagging offences where information is obtained by deceiving organizations who holds it.

Management of Information Security Incidents and Improvements

A consistent approach to dealing with all data security events must be maintained across the Council. Such events must be analysed, and the SIRO must be consulted, for the Head of Service/Managing Director to establish when a security event should be escalated to an information security incident. The incident response procedure must be a seamless continuation of the event reporting process and must include contingency plans to advise the Council on continuing operation during the incident.

Collection of Evidence

If an incident requires information to be collected for an investigation, strict rules need to be adhered to. On no account should managers attempt to investigate incidents themselves. They should refer them to the appropriate officers in accordance with the Councils Data Protection Policy and Anti Fraud and Corruption Strategy and Disciplinary Procedures etc.

Responsibilities and Procedures

Management responsibilities and appropriate procedures are established to ensure an effective response against security events. When an incident is discovered the Head of Service/Managing Director must be informed immediately. The SIRO must advise the Head of Service/Managing Director so they may determine the most appropriate response.

An incident management record must be created and include details of:

- Identification of the incident, analysis to ascertain its cause and vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the Council to those affected.

The actions required to recover from the security incident must be under the control of the Head of Service/Managing Director. Only identified and authorised staff should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible

Learning from Information Security Incidents

To learn from incidents and improve the response process, a Post Incident Review must be conducted. The following details must be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.

The information must be collated and reviewed on a regular basis by ICT and any patterns or trends identified. Any changes to the process made as a result of the Post Incident Review must be formally noted.

Information Commissioner's Office

Although there is no legal obligation in the DPA for data controllers to report breaches of security which result in loss, release or corruption of personal data, the IC believes that serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA.

"Serious breaches" are not defined. However, in considering whether breaches should be reported you need to take into account the potential harm to data subjects, the volume of personal data lost and the sensitivity of the data.

There is a presumption that the matter should be reported where a large volume of personal data is concerned and there is a real risk to individuals suffering some harm.

However, it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high due to the circumstances of the loss or the extent of information about an individual.

The Head of Service/Managing Director shall, in consultation with the SIRO, shall determine whether to report the data security incident to the ICO.

Serious breaches should be notified to the ICO by email using the address casework@ico.gsi.gov.uk or by post to Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Further guidance on how to manage a data security breach can be found on the Information Commissioners website:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.ashx

WLBC DP GUIDANCE NOTE 14

Government Connect

Government Connect is a national program which is intended to provide a way for authorities to exchange information with each other, central government, the police, NHS etc in a secure, authenticated way.

The Council is linked to the Government Connect GCSx network for the transferring of sensitive or restricted information between the authority and other local authorities and government departments. To ensure compliance, the Council must comply with the requirements of Government Connect.

Officers who handle sensitive or restricted information as categorised by Government Connect must be made aware by their line manager of the impact of the loss of such material and the actions to take in the event of such a loss. The criteria for assessing sensitive information includes anything that may:

- Cause substantial distress to individuals
- Cause financial loss or to facilitate improper gain or advantage for individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Breach undertakings to maintain the confidence of information provided by third parties
- Undermine the proper management of public sector and its operation.

A more detailed explanation of these criteria can be found at: www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx

Each user of the network connected to GCSx who has regular access to sensitive information or information that originates from the Government Secure Intranet (GSI) MUST be at least cleared to the Baseline Personal Security Standard (BS). Whilst BS is not formal security clearance, BS provides a level of assurance to the trustworthiness and integrity and probable reliability of prospective employees. A BS check involves verification of: identity, last 3 years employment history, nationality and immigration status and criminal record (unspent convictions only). Contact the HR team for further information

If an officer requires access to the GCSx network, then they must sign the GCSx Acceptable Use policy below:

WLBC GCSx Acceptable Usage Policy

I understand and agree to comply with the security rules of West Lancashire Borough Council as well as the GSi CoCo.

For the avoidance of doubt, the security rules relating to secure e-mail and ICT systems usage include:

I acknowledge that my use of the GSi may be monitored and/or recorded for lawful purposes;

I agree to be responsible for any use by me of the GSi using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and

will not use a colleague's credentials to access the GSi and will equally ensure that my credentials are not shared and are protected against misuse;

and will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and

will not attempt to access any computer system that I have not been given explicit permission to access;

and will not attempt to access the GSi other than from IT systems and locations which I have been explicitly authorised to use for this purpose; and

will not transmit information via the GSi that I know, suspect or have been advised is of a higher level of sensitivity than my GSi domain is designed to carry; and

will not transmit information via the GSi that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and

will not make false claims or denials relating to my use of the GSi (e.g. falsely denying that an e-mail had been sent or received); and

will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GSi to the same level as I would paper copies of similar material; and

will not send Protectively Marked information over public networks such as the Internet; and

will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain; and

will not auto-forward email from my GSi account to any other non-GSi email account; and

will disclose information received via the GSi only on a 'need to know' basis; and

will not forward or disclose any sensitive or protectively marked material received via the GSi unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and

will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GSi (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted; and

will securely store or destroy any printed material; and

will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GSi (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc., so as to require a user logon for activation); and

where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection; and
will make myself familiar with the security policies, procedures and any special instructions that relate to the GSi; and

will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and

will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and

will not remove equipment or information from my employer's premises without appropriate approval; and

will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief); and

will not introduce viruses, Trojan horses or other malware into the system or GSi; and
will not disable anti-virus protection provided at my computer; and

will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and

if I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Signed: _____ Date: _____