Information Governance and Security Policy

Version and Review Summary

Rev	Date	Author	Approver	Revision description
1.00	November 2012	Tony Monachello		Formal Review Ratified at Information Governance Board January 2013
2.00	March 2014	Tony Monachello		Formal Review Ratified at Information Governance Board 19th March 2014

1. Purpose

The council holds information in many forms such as paper files, computer records, audio recordings, photographs and movie images. These are known as 'Information Assets'.

It is important that these assets are properly protected for the following reasons:

- We need to assure our residents, staff and other stakeholders that their information is secure;
- We have to satisfy legal requirements and can be fined heavily if we fail;
- Loss of data would be reputationally damaging for the council.

Good management of information assets is a key enabler for information sharing to support:

- Access channel strategy;
- Business continuity planning;
- Citizen focussed services;
- Flexible working.

Information may be processed and stored on computers or in other electronic form, printed or written on paper, shared through voice or video communications, transmitted through post or electronic means such as e-mail or fax, made available on corporate videos or web sites. Whatever form the information may take, or means by which it is shared, stored or processed, it should always be appropriately classified and protected according to that classification.

This policy sets out how information assets are governed and secured.

2. Policy Definition and Scope

Standards[1] for information security cover three areas:

1. **Confidentiality**: Information is only available to those that are authorised to gain access.

2. **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.

3. **Availability:** The assurance that authorised users have access to information and associated assets when this is required.

We need to be particularly concerned with the controls surrounding **sensitive data**. This type of data may contain:

- Personal/sensitive information, as defined by the Data Protection Act 1998;
- Health information;
- Customer record information;
- Card holder data;
- Commercially sensitive documents;
- Any information that is protected by council policy from unauthorised access.

[1] The Data Protection Act, Local Government Association Guidelines and the ISO 27001 Code of Practice.

3. Information Governance Assurance Roles

Information Governance is assured through the specific roles detailed below.

- *The Accounting Officer* (Head of Paid Service - HPS) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

- *The Senior Information Risk Owner (SIRO) is the Information Governance Lead* with delegated authority from the HPS. The SIRO provides assurances to the HPS on the controls & procedures for managing information and chairs the council's Information Governance Board.

- *The Information Governance Board (IGB)* will be represented by all levels of management to provide visible management support and clear direction for information security at the executive level.

- *The Caldicott Guardian* has a specific set of responsibilities for defining the circumstances in which social care and childrens personal information can be legitimately shared with other council departments and outside agencies.

- *Information Asset Owners (IAOs)* are responsible for ensuring that information risk is managed appropriately and for providing assurances to the IGB and the SIRO. This will include business continuity plans for information that is deemed to be critical.

- *Information Asset Controllers (IACs)* support the IAOs and are responsible for managing risks to information assets within their respective service area.

- *Business Transformation Client Team* will act as the focus for all Information security issues, suggesting policies to mitigate risk, and assisting with their interpretation into team procedures and standards, whilst implementing those aspects affecting the operational security of the council's information and IT infrastructure.

The following diagram summarises the information governance structure:

Structural Model	Harrow Council
Accounting Officer	Head of Paid Services
SIRO	Corporate Director of Resources
Information Asset Owner (IAO)	Corporate Directors/Divisional Directors
Information Asset Controller (IAC)	Divisional Directors/Service Managers

4. Information Governance Responsibilities & Guidance

Governance of information assets is the responsibility of all staff and managers, as well as the designated Information Governance assurance roles defined in the previous section. This section describes those responsibilities and the documents which define them. Service areas will also need to hold local policies and procedures relating to the management and handling of their specific information assets.

Acceptable Use **-** All staff that have been issued with a user ID/password to access council systems are required to sign up to the **Acceptable Use Policy (Appendix 1).** The policy summarises all staff responsibilities in relation to information assets. It is recommended that managers remind staff on an annual basis of their information governance responsibilities. Access to Council IT systems will only be provided on signature and acceptance of this policy.

Data Security Training **-** All staff that have been issued with a user ID/password to access council systems are required to undertake the on-line *Learning Pool* 'Introduction to Data Security' training module on an *annual* basis.

Secure Transmission **-** Staff will only transmit sensitive data using an approved encrypted process **(Appendix 2, Secure Transmission of Sensitive Data).**

Personal Data **-** The Council recognises its duty – as custodians of personal data – to ensure that it is handled properly and in accordance with the law at all times **(Appendix 3, The Council's Data Protection Policy).** Operational implications of this policy are addressed in other policies and guidelines, which are attached to this policy as appendices.

Records Management **-** Information Asset Owners will manage the storage, retention and availability of their information assets in accordance with **Information and Records Management Policy (Appendix 4).**

Data Breaches **-** Managers will take appropriate steps to prevent, detect, and recover from any loss or incident, whether accidental or malicious, including error, fraud, misuse, damage and disruption to, or loss of computing or communications facilities **(Appendix 5, Incident Reporting guidelines).**

Data Sharing **–** Staff sharing data with 3rd parties and internal officers must adhere to all sharing guidelines and any required code of connection protocols **(Appendix 6, Third Party Data Sharing Guidelines, Appendix 7, Confidentiality Guidelines, Appendix 8, Internal Information Sharing Protocol & Appendix 9, Third Party Code of Connection).**

Monitoring and Disciplinary Action

The Council proactively monitors the use of Information Assets including its IT Systems. Any *actual or suspected breaches of this Policy* within, or affecting the Council's systems or information (electronic or manual based) will be dealt with under the Council's Disciplinary Procedure.

5. Review of Policy

The Information Governance Board (IGB) will review this policy on a yearly basis, and the results of the review will be detailed on the minutes of this meeting. Any resulting changes will be reflected in a revised version of this policy and notified to all relevant stakeholders.

In the event of major network configuration changes, change of policy, security incidents or a lack of security identified in the yearly penetration test performed on the Council's network, the policy will be reviewed for effectiveness, and modified if appropriate.

6. Exceptions to Policy

Any deviation to this policy must be submitted in writing to the Business Transformation Client Team and will only be approved in **exceptional** circumstances. All decisions will be confirmed in writing by the Client Team.

Appendix 1

Information and Systems Acceptable Use Policy

The policy has been issued in conjunction with the Council's Information Governance & Security Policy and is **mandatory for all users** of Harrow information or information systems including members, employees, temporary workers, contractors and any authorised 3rd parties (except where a 3rd party acceptable use policy is in existence and is covered as part of a data sharing agreement). Further details in relation to this policy can be found in the *Information Management* section of the hub.

The Council proactively monitors the use of Information Assets including its IT Systems. Any ***actual or suspected breaches*** *of this Policy* within, or affecting the Council's systems or information (electronic or manual based) will be dealt with under the Council's Disciplinary Procedure.

1. My Responsibilities

- I will undertake on-line information security training annually and will familiarise myself with the council's Information Governance & Security policy and guidelines.

- I am responsible for the security of my data and will clearly label the sensitivity of that data to others that I share it with: the email or document header should include the label *"OFFICIAL -SENSITIVE"* when contents are of a SENSITIVE nature. See '*Protective Marking"* guidance for more information.

- I understand that the Council's IT equipment and systems are provided for business use and that only limited personal use of email and the internet is acceptable.

- I will not access any data or systems unless I have a business need and have been authorised to do so.

- I will not store council data on non-council devices or external storage/email systems unless specifically approved in writing by the council's Client Team.

- I am responsible for the use of my user ID/password and e-mail address; in particular, I will not write down or share my password.

- I will use strong and secure passwords (8 or more characters, upper/lower, numeric and including special characters such as £%&) to protect the data that I work with.

- I will not use a colleague's user ID/password to access the council's network or information systems.

- I will not leave my council computer, laptop or any other device unattended in such a state as to risk unauthorised viewing of information displayed on it. Whilst working on my device (in the office or remotely) I will take precautionary measures to prevent unauthorised disclosure of data through "shoulder surfing" i.e. someone looking over my shoulder to view information that they have no right to read.

- I will ensure that I either 'power off' or 'lock' my device when leaving it unattended.

- I will take reasonable precautions to secure my council laptop, phone and any other mobile device, locking it away and storing it out of sight when unattended. I will ensure that documents left in unattended vehicles are out of sight and locked away securely in the boot. I will never leave council paperwork or mobile devices in any vehicle overnight.

- I will not remove business data from council systems unless I have a valid business reason to do so.

- I will never take or send SENSITIVE information out of the office on removable media unless it has been encrypted using council approved systems/mechanisms.

- I will treat **all personal data** as defined by the Data Protection Act as *OFFICIAL SENSITIVE.*

- I will not view or transport NHS SENSITIVE data (also known as PID) outside of England.

- I will inform my line manager and the IT Service Desk (x2000) immediately if **a)** I detect, suspect or witness an incident that may be a breach of information security, **b)** I suspect that my workstation or laptop has been infected by a virus or malicious code or **c)** my council device or papers are lost or stolen.

2. **I Will Use Email, Instant Messaging (Lync) and Conversations (SharePoint Newsfeeds) Responsibly.**

- I will always use professional and appropriate language in all messages and conversations.

- I will not use any language or post messages (including images) that are abusive, threatening, harassing, discriminatory or otherwise offensive. This includes forwarding any received email. If I receive any messages of this nature from another employee or other outside organisations, I will inform my line manager immediately.

- I understand that when sending emails of a SENSITIVE nature to external email addresses, the use of GCSx, CJSM, Egress Switch systems or any other council approved encryption method is mandatory, to ensure that the email is secured.

- I will only use the council's official corporate email account to conduct council business.

- I will never send an email containing business or SENSITIVE information to my personal email account in order for me to work from home (and vice versa, personal email to office email).

- When emailing or replying to Members I must ensure that I am doing so to their *"harrow.gov.uk"* email and not their personal email account. Certain nominated officers may send (at their discretion) **non-sensitive** information to a Members' personal email address. Full details of nominated officers can be found here.

3. I Will Use the Internet Responsibly

- I will not visit web sites that are obscene, hateful, pornographic or otherwise illegal material. If I do so inadvertently I will advise my line manager immediately.

- I will not visit any gambling sites, participate in any on-line games or have active any web channels that broadcast frequent updates to my PC/device.

4. When in the Office, I Will Ensure That Sensitive Paper Documents Are Kept Safe

- I will keep SENSITIVE documentation in secure storage.
- I will always observe a clear desk policy when dealing with SENSITIVE information and ensure that it is not left on my desk unattended.
- I will always dispose of unwanted paper (SENSITIVE or non-SENSITIVE) in the secure paper waste bins provided.
- I will always collect SENSITIVE information straightaway when printing.
- If I am faxing SENSITIVE information, I will use the 'Safe Haven' process when doing so. After confirming the fax number to be used, I will ask the intended recipient to stand by their fax machine until the document has been received.
- If I am required to send SENSITIVE information via conventional post, I will ensure that registered or recorded delivery mechanisms are used.

5. I Will Manage Additional Risks of Working Remotely

- If I have to take SENSITIVE documents out of the office, I will ensure that they are transported securely. I will take reasonable precautions to secure the documents, locking them away and storing out of sight when unattended.
- Any council paperwork I take off site and subsequently no longer required, I will shred (cross cut) or return to the office to be disposed of appropriately.
- I will only use approved secure remote access systems when performing remote working.
- I will only access council data or systems using business provisioned 'managed' devices.
- I will not access any sensitive data or systems over open wi-fi or from Internet Cafés.
- I will only access government secure systems such as GCSx from a council managed device on council premises.

6. I Will Use the Council's Approved Technology Services

- I will only purchase computers, phones, and any other portable devices capable of storing data through the council's approved procurement channels.
- I will not install or configure software (including freeware, music, video files, personal data, photos etc) or peripherals, including enabling Wi-Fi on routers. All changes are to be undertaken by the council's technology partner.
- I will not store data on 3rd party sites or the Internet cloud services.
- I understand that the business use of social media sites must be agreed by the Communications Team and I must follow/sign up to the council's Social Media Protocol.

7. I Will Handle Payment Card Information Securely

- If I handle payment card data, I will not make ad-hoc notes of card numbers or send card information via e-mail.

- I will not write the card verification number (3 digits at back of card) down or type it into any electronic system other than the one used for making payments.

- I will not copy, move, or store payment card information onto local hard drives, network drives, voicemails or removable electronic media.

- If I receive credit card details by email I will respond (erasing all credit card details) stating that the council does not accept payment details by email, advising them of the appropriate payment channels. I will then delete the original email from my in-box and Trash folder.

- If I receive any credit card details by letter, I will write to the sender advising them of the appropriate payment channels. I will then destroy the original letter by placing in the council's secure paper waste bin or console ready for shredding.

- If I am a custodian of a portable *Chip and Pin* device I will ensure that they are securely stored when not in use.

- I will not attempt to enter PIN details into a *Chip and Pin* device for a service user even if he/she is willing to supply me with the PIN number voluntary.

Appendix 2

Secure Transmission of Sensitive Data

Sensitive data should always be transmitted using an approved encrypted process. If you are an authorised user of the Government Connect Secure Extranet (GCSx), the Criminal Justice System Mail (CJSM) or Egress Switch, you must use them (in accordance with the terms and conditions of the relevant system) to transmit sensitive data. Otherwise please follow the file encryption procedures below:

- Launch 7-zip using the **Start menu** (Start - All Programs - 7-zip - 7-zip file manager).
- In the 7-zip file manager locate the file that you want to encrypt.
- Once you have located the file you want to encrypt, select it by clicking it once.
- With the file highlighted, click '**Add**.'
- This will open a new window called '**Add to Archive**.'
- At the top of the left column change the '**Archive Format'** to '**Zip**' using the drop-down menu.
- At the bottom of the right column check that the 'Encryption method' says '**AES 256**.'
- Above it, type your chosen password into the '**Enter password'** text box.
- Directly beneath it, re-enter password into to the '**re-enter password'** text box.
- Please make sure that the '**show password**' field is NOT ticked.
- Click '**OK**' to close the '**Add to Archive'** window.'
- Back in the file manager you can now see the encrypted and zipped file. You can identify it by its icon, which is of a folder with a zip through it. You may need to use **Ctrl + R** to refresh the screen.
- You can now send the file as an email attachment but remember **NOT** to include the password in the same email.

Opening an encrypted file:

- In the email message window right click the zipped attachment.
- Choose the 'save as' option and save it to your desired location on your computer.
- Click '**Save**.'
- Close the email message window.
- Open 7-zip using the **Start menu**. This will open the 7-zip file manager.
- Browse for your encrypted file using the drop down list of file locations.
- Once you have located your file double click it to open the folder.
- In the folder, select **extract** or **double click** the required document to open it.
- At this point you will be asked to enter the password assigned to the encryption process.
- Enter the password and click '**OK**.'
- The document should open.

Best Practice for Password Setting:

- Make passwords hard to guess (8-12 characters in length, alphanumeric with at least one capital letter and at least one symbol include some special characters like - %$£).
- NEVER send out passwords in the same email as the encrypted file(s).
- **Always confirm** the identity of the recipient before releasing passwords.
- Inform recipients of passwords either face to face or by telephone (where possible).

Appendix 3

Data Protection Policy

Data Protection Policy

Introduction

Harrow Council is fully committed to compliance with the requirements of the Data Protection Act 1998 (the "Act"), which came into force on the 1st March 2000. The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, the Council has to collect and use information about people with whom it works or provides services to. These include members of the public, elected members, current, past and prospective employees, clients and customers, and suppliers. In addition, the Council may be required by law to collect and use personal information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

The Council regards the fair and lawful treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information fairly and lawfully.

To this end the Council will comply with the Data Protection Principles set out in Part 1 of Schedule 1 of the Act. Any breach of this Data Protection Policy or the Act will automatically be considered a breach of discipline and existing Council disciplinary proceedings may apply.

The Principles of Data Protection

The Act stipulates that anyone processing personal data (the "data processor") must comply with **Eight Principles** of good practice. These Data Protection Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;

7. Shall be kept secure i.e. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Personal Data and Sensitive Personal Data

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and **"sensitive"** personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data; includes name, address, telephone number, id number, date of birth etc
- That data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive personal information

The Council will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Specify the purpose for which the Council will use personal information;
- Collect and process personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure that the personal information it processes is accurate and up to date;
- Apply checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;

- Ensure that the rights of people about whom the information is held ("data subjects") can be fully exercised under the Act. These include:

    - The right to be informed that processing is being undertaken;
    - The right of access to one's personal information within 40 days;
    - The right to prevent processing in certain circumstances;
    - The right to correct, rectify, block, have noted any information that the data subject regards as incorrect or erase information regarded as wrong information.

In addition, the Council will ensure that:

- There is someone with specific responsibility for data protection in the Council;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information will be regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out in accordance with the Data Protection Principles. Any disclosure of personal data will be in compliance with approved procedures.

Management and Staff Responsibilities

All managers and staff within the Council will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

Contractors' Responsibilities

All contractors, consultants, partners or other servants or agents of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm;
- Allow data protection audits by the Council of data held on its behalf (if requested);
- Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages.

All contractors who process personal information supplied by the Council will be required to confirm that they will abide by the requirements of the Act with regard to personal information supplied by the Council.

Caldicott Guardian

The Caldicott Guardian has a specific set of responsibilities for defining the circumstances in which personal information held about clients can be legitimately shared with other Harrow departments and with other agencies. In Harrow, the Caldicott Guardian's responsibilities primarily relate to adults & children services. The Guardian is also responsible for ensuring that these information-sharing guidelines are publicised appropriately and strictly adhered to.

Implementation

The council will appoint a Data Protection Manager (Service Manager, Information Management). Designated officers will also be identified in all directorates (see hub for details). These officers will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Data Protection Manager who will also have overall responsibility for:

- The provision of data protection training for staff within the Council.
- The development of best practice guidelines.
- Carrying out compliance checks to ensure adherence throughout the Council with the Act.
- Provision of professional support, updates and advice to officers on data protection and related matters
- Notification to the Information Commissioner

Breaches of the DPA

All breaches of the DPA must be reported to the council's client team who will record the incident into the corporate breaches register. An incident form must then be completed by the originating directorate with the details of the incident, actions taken since the incident and any controls put in place to ensure that the incident is not repeated (see Appendix 5, Incident Reporting).

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Harrow Council is registered as the Act requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. To this end the designated officers will be responsible for notifying and updating the Data Protection Manager of the processing of personal data, within their directorate.

The Data Protection Manager will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner within 28 days.

To this end any changes made between reviews will be brought to the attention of the Data Protection Manager immediately.

Review of Data Protection Policy

The Information Governance Board (IGB) will review this policy on a yearly basis, and the results of the review will be detailed on the minutes of this meeting. Any resulting changes will be notified to all relevant stakeholders.

Appendix 4

Information and Records Management Policy

1. Introduction

The Council creates and receives a variety of information as part of its day-to-day business and activities. Having accurate, relevant and accessible information is vital to the efficient management of the Council's business functions.

Good management of records, and information contained within them, benefits the Council through:

- Understanding the importance of our information and the risks to it
- Information being easily and efficiently located, accessed and retrieved
- Information being better protected and stored more securely
- Information being disposed of safely and at the right time

In addition, the Freedom of Information Act 2000 and the Data Protection Act 1998 put greater emphasis on the Council's ability to make information available to the public and set out specific requirements for the creation and management of information and records (including "open" data initiatives - that the data is free to access, use and reuse and is available via the internet).

The council is committed to open government and the pro-active release of the information it holds. We must therefore balance its statutory obligations, for example, providing the public with access to information with the aim of being open and transparent without compromising its confidentiality. We will be open and transparent with all data by default, increasing the amount of open data published over time. This includes Freedom of Information (FOI) requests which will be published as open data on the council's web pages.

2. Purpose

The purpose of this policy is to ensure that all Harrow Council staff and other users of Council's information understand what they must do to manage and protect information and records effectively, efficiently, and economically.

Good information and records management relies on the following principles being applied:

- Regular review of information held
- Organise at point of creation
- Keep safe and secure
- Dispose when no longer required

3. Scope

This policy applies to all Council staff, partners, contractors, suppliers and any other third party that use or create Council information and records regardless of the format or media in which they are held in, for example.

- Documents (including written or typed word documents)
- Letters
- Forms
- Paper based files
- Databases, spreadsheets, presentations

- Electronic forms and emails
- Diaries
- Reports
- Audio and video tapes including CCTV
- Microfiche and microfilm
- Maps and plan
- Photographs
- Brochures
- Intranet and internet pages

4. Key Principles

The following principles will apply to Council information and records regardless of its format:

- Where practicable, information and records will be accessible to all Council staff and members of the pubic, unless there is an explicit business reason for access to be limited.
- A consistent approach will be adopted with regard to the creation, storage, retrieval, archiving, and disposal of information and records.
- Information and records will be stored within a filing structure that reflects the Council's business functions rather than hierarchical or organisational structure.
- The management of information will be in accordance with the Council's Information Governance and Security Policy and comply with legal requirements.
- All Staff will create and maintain full and accurate information records of all council activities and transactions.
- All information and records will be captured and managed within the appropriate information and records management systems.
- Email will only be used as means of transmission and not for storage.
- Staff will not store information in individual filing systems or on their hard drive (i.e. my documents or desktop).
- Staff will work towards protectively marking and labelling information.
- Information and records will not be retained, distributed or copied unnecessarily.
- Information and records will be disposed of appropriately when longer required and only by authorised staff

Appendix 5

Incident Reporting

Management & Risk Recovery Procedure

Purpose

The purpose of this document is to describe the procedures for identifying, reporting, responding to, and learning from security incidents, threats or vulnerabilities whether actual, suspected or perceived.

Scope

This procedure is applicable to all aspects of the Council's operations whether electronic, non-electronic, personnel, premises or infrastructure.

Overview

All systems and activities will be subject to formal incident recording and escalation procedures.

Incident recording will be used to log all unusual events. This mechanism will include what happened, what was done and final resolution.

The objective of Security Incident Reporting and Management is to detect, investigate and resolve any actual, suspected or potential breaches of security, and to take action that will avoid, or reduce the impact or probability of a further similar reoccurrence.

A security incident is an event which causes or has the potential to cause:

- Degraded system integrity.
- Loss of system or information availability.
- Disclosure of confidential information, whether electronic or paper, or any other form including conversation.
- Corruption of information.
- Disruption of activity.
- Financial loss.
- Legal action.
- Unauthorised access to applications.
- Unauthorised access to premises.

Examples of incidents could include activity such as:

- Attempts (either failed or successful) to gain unauthorised access to a system or its data
- Unwanted disruption or denial of service.
- The unauthorised use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- Loss of removable media (Encrypted USB Stick, Disc etc) and portable equipment (Laptops/Tablet PCs).
- Tampering/attempting to tamper with CCTV cameras or the leaking of unauthorised film footage taken from CCTV equipment.
- Loss of paper files containing sensitive data.

While each employee is personally responsible for ensuring that no security breaches occur as a result of their actions, everyone must be aware of their responsibility to report any potential, suspected or actual incident such as security threats, data loss, vulnerabilities, breaches, software or system failures to Capita, who in conjunction with the Client Team will check the validity and severity of the incident and respond accordingly, taking whatever action is required. Where relevant, the change control process will be followed.

Security breaches caused knowingly, by reckless behavior, or non-compliance with information security policies including the non-reporting of an incident, may result in disciplinary action.

Responsibilities

Users

- Report any data security incidents promptly to IT Service Desk x2000.
- Any employee who suspects that his/her workstation or laptop has been infected by a virus or malicious code shall IMMEDIATELY call the IT Service Desk.
- Complete Security Incident Report Form (available on Hub or please see Attachment A) and return via email to **itclient.team@harrow.gov.uk**
- **Appropriate Line Manager** to instigate management and recovery plan protocols (attachment D) and to manage activities required to avoid or reduce the probability of reoccurrence and the potential impact of future incidents.
- Provide further information or evidence when requested.

Capita IT Service Desk

- Allocate call log reference.
- Assign to appropriate queue and advise the Client Team immediately. Please be aware that not all incidents are to be assigned to the "security incident" queue as in some cases the incident needs to be resolved by the appropriate Capita technical team (i.e. in the case of a DoS attack).

Client Team

- Allocate severity and priority to the incident and agree resolution action plan.
- Monitor resolution of the related incidents.
- Advise and involve other parties as appropriate, including escalation within the Council. Other parties may include emergency response teams *UNIRAS, NISCC, NHTCU.*
- Add incident to corporate breaches register.
- Review resolved incident.
- Provide quarterly reports of incidents to the Information Governance Board (IGB)/SIRO.

- If appropriate, advise the Information Security for London (ISfL) forum who are the London WARP (Warning, Advice and Reporting Point) isfl.incidents@ktac.nlawarp.gov.uk. If the matter is more of a sensitive nature please inform the ISFL Group Manager first matt.smith@isfl.org.uk.
- Inform Legal Services (if appropriate). In the event of data loss or breach, confirm with Legal if the Information Commissioner's Office is to be informed.
- Inform the Council's Insurance Team (if appropriate)
- Advise the Communications team of any potential data loss or breach. While it is difficult to determine in advance what level of detail to provide to the press, some guidelines to keep in mind are:

    - Keep the technical level of detail low.
    - Detailed information about the incident may provide enough information for copycat events or even damage the site's ability to prosecute once the event is over.
    - Keep the speculation out of press statements. Speculation about who is causing the incident or the motives may cause misinformation which could lead to legal challenge.
    - Work with law enforcement professionals to assure that evidence is protected. If prosecution is involved, assure that the evidence collected is not divulged to the press.
    - Try not to be forced into a press interview before you are prepared.
    - Do not allow the press attention to detract from the handling of the event. Always remember that the successful closure of an incident is of primary importance.

Service Manager, Information Management

- Approve closure of resolved incidents.

Recording

Every reported incident will be recorded on a Security Incident Report form (Attachment A) and the council's data security breaches register.

The IT Service Desk will allocate a call reference number and inform the relevant resolution team immediately.

Procedure

This section describes the procedure, but as every incident is different, common sense should be used to ensure that incidents are resolved with appropriate priority according to their severity.

Prompt action may be necessary to reduce the potential impact of an incident, so there may be times when an incident is resolved before it is recorded. If this occurs, an incident report form should be completed as soon as possible after the event.

It is important that every incident, however minor is recorded and follows this procedure to ensure that the probability of reoccurrence is avoided or reduced, and the impact of future incidents is minimised. (See Attachment D for further information).

Resolution

Once the incident has been recorded, it will be prioritised according to severity, which will be based upon the actual or potential impact of the incident upon the Council's systems and information and will be categorised as:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

Resolution of the incident will be allocated to an individual or team, and an action plan will be produced with target resolution times. The resources used to resolve the incident will depend upon the identified severity level, for example in the case of a Low severity "no action" may be an acceptable option if the resources required outweigh the impact.

The Client Team will monitor the resolution, and the reporting users should be kept advised of progress.

Escalation

Every security incident that may have an impact on the Council or its customers will be reported immediately to Service Desk and the Client Team in order to ensure that appropriate priority and resources are allocated to resolving the incident. The **Client Team in turn will contact the following officers/originations** if appropriate:

- The relevant senior officers within the Council.
- Communications Team. **Direct dial:** 020 8424 1857 **Ext:** 2857
- If appropriate the Information Commissioner (see Attachment B)
- If appropriate inform the council's Warning, Advice and Reporting Point (WARP) isfl.incidents@ktac.nlawarp.gov.uk. If the matter is more of a sensitive nature please inform the ISFL Group Manager first matt.smith@isfl.org.uk
- If appropriate inform CJSM, the Criminal justice system (i.e. if a virus was to effect the criminal justice secure eMail system directly) then contact CJSM with details at CJSM Service desk on **0870 010 8535** between 08:00 and 19:00 Monday to Friday, or email: cjsm.helpdesk@vodafone.com
- If appropriate inform the PSN (Public Services Network). PSN provides an assured network over which government can safely share services. psna.servicebridge@cabinet-office.gsi.gov.uk. Further details on incident reporting to PSN can be found in the incident section on the PSN website.
- If appropriate *GovCertUK* (see Attachment C). The incident will first be reported to ISfL and if the need arises escalated to GovCertUK (a body that assists government departments and organisations in the recovery from a computer security incident) using the appropriate reporting template (see Attachment E) and emailed to incidents@govcertuk.gov.uk. Further details can be found at http://www.govcertuk.gov.uk/reporting-an-incident.shtml

Review and learning

All resolved incidents will be reviewed to ascertain whether there is a risk of reoccurrence. If there is no such risk the incident record will be closed. All potential vulnerabilities will be assessed, and appropriate action taken to ensure that the risk is kept to an acceptable level, implementing such controls as may be necessary.

If appropriate risk registers for IT and Information Management will be updated.

Closure

Each incident will remain open until it has been satisfactorily resolved, documentation completed, and actions taken to avoid reoccurrence, or to ensure the impact of reoccurrence is at an acceptable level. Closure is only be approved by the Service Manager, Information Management.

Attachment A - INCIDENT REPORTING FORM (to be completed by Line Manager)

Service Desk Ref No: -	

Nature of incident: -			
Systems or information affected			
Department affected: -			
Notified By: -		Date: -	
Allocated to: -		Date: -	
Description of Incident and impact: -			
Severity: C/H/M/L			
Summary of Findings and action plan: -			
Review and actions taken to avoid reoccurrence (include key controls to ensure incident does not happen again): -			
How have relevant staff been notified of any changes to working practices as a result of the incident?			
What evidence are you providing to support notification to staff?			
Have your staff undertaken the *mandatory* on-line information security training (in particular all staff who have had a direct involvement in this incident)?			
Date Closed: -			
Signed: **Service Manager, Information Management**			

Attachment B - Notification of Data Security Breaches to the Information Commissioner's Office

Although there is no legal obligation on data controllers to report breaches of security, which result in loss, release or corruption of personal data, the Information Commissioner believes 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 the following should assist data controllers in considering whether breaches should be reported:

The potential harm to data subjects:

The potential harm to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the Information Commissioner's Office.

Ways in which harm can occur include:

- Exposure to identity theft through the release of non-public identifiers e.g. passport number.

- Information about the private aspects of a person's life becoming known to others e.g. financial circumstances.

The extent of harm, which can include distress, is dependant on both the volume of personal data involved and the sensitivity of the data.

Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

Where there is little risk that individuals would suffer significant harm, for example because a stolen laptop is properly encrypted, or the information that is the subject of the breach is publicly available information, there is no need to report.

The volume of personal data lost / released / corrupted:

There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise what constitutes a large volume of personal data. Every case must be considered on its own merits but a reasonable rule of thumb is any collection containing information about 1000 or more individuals.

An example the ICO would expect to be reported would be the theft / loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic / digital media holding names and addresses, dates of birth and National Insurance Numbers of 1000 individuals.

An example the ICO would not expect to be reported would be the theft / loss of a marketing list of 500 names and addresses or other contact details where there is no particular sensitivity of the product being marketed.

However it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether to report or not, then the presumption should be to report.

The sensitivity of the data lost / released / unlawfully corrupted:

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is *sensitive personal data* as defined in section 2 of the DPA. As few as 10 records could be the trigger if the information is particularly sensitive.

An example the ICO would expect to be reported would be a manual paper based filing system (or *unencrypted* digital media) holding the personal data relating to 50 named individuals and their financial records.

An example they would not expect to be reported would be a similar system holding the trade union subscription records of the same number of individuals where there were no special circumstances surrounding the loss.

Serious breaches will be reported (by the Legal and/or the Client Team) to the Information Commissioner's Office at **casework@ico.gsi.gov.uk** or at Address: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.* The notification should include:

- The type of information and number of records.
- The circumstances of the loss / release / corruption
- Action taken to minimise / mitigate effect on individuals involved including whether they have been informed.
- Details of how the breach is being investigated.
- Whether any other regulatory body has been informed and their response.
- Remedial action taken to prevent future occurrence.
- Any other information.

Attachment C - Guidance for Reporting Electronic Attack Incidents

Introduction

From the first of February 2007 CESG, as the National Technical authority for Information Assurance (IA), has assumed the lead responsibility within UK Government for providing IA advice to public sector organisations. This role includes providing an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents. Prior to that, the National Infrastructure Security Coordination Centre (NISCC) provided incident response to Government and the Critical National Infrastructure (CNI) via its CERT team UNIRAS.

To facilitate the provision of incident response operations to Government, CESG has formed a dedicated team to operate a CERT (Computer Emergency Response Team) function, with this team being identified to the Government community as GovCertUK.

The CESG GovCertUK Incident Response team provides a 24/7 (24 hours 7 days a week) operation, and can be contacted on the following:

Telephone: 01242 709311

Fax: 01242 709113

General Enquiries: enquiries@govcertuk.gov.uk or govcertuk@cesg.gsi.gov.uk

Incidents & Alerts: incidents@govcertuk.gov.uk or govcertuk@cesg.gsi.gov.uk

During Office hours 0830hrs – 1700hrs all correspondence will be monitored by the GovCertUK response team. Outside office hours, weekends, and public holidays, all correspondence will be monitored by a duty officer, supported by on-call GovCertUK response personnel

One of CESG's roles is to minimize the risk and effects of electronic attack to the Government community. As CESG's Computer Emergency Response Team, GovCertUK assists Government departments and organisations in the recovery from a computer security incident. They gather data from all available sources to monitor the general threat level and focus. For these reasons the early reporting of incidents and attempted attacks is highly recommended

To assist in the identification and categorisation of an event please read GovCertUK's Incident Response Guidelines (pdf) for further information and guidance.

Reporting Process

Incidents should be reported on direct on telephone number 01242 709311 for an initial response, which should be followed up with an email to incidents@govcertuk.gov.uk using the incident template (doc) (Attachment E)

During office hours (0830 -1700) all correspondence is monitored by the GovCertUK response team. Outside office hours, at weekends and on public holidays all correspondence will be monitored by a non-specialist duty officer, supported by on-call GovCertUK response personnel. When speaking to the duty officer, please be clear that the call is for GovCertUK

Where possible as much supporting information as possible should be supplied, such as log files, internal/external IP addresses, affected Operating Systems, patch levels and policy etc.

How to submit Malware samples to GovCertUK

All samples should be sent by carefully following the procedures below:

- All samples should be renamed to <origninalfilename>.<orginalfileextension>.txt
- All samples should then be zipped and password protected with the password 'infected'
- Optionally (but recommended), PGP encrypt the message (and attachments) with the GovCertUK Public Key, available here
- Use the following subject line: 'MALWARE SAMPLE'
- Send the message to samples@govcertuk.gov.uk

NB: To submit Malware samples that are classified, are from classified systems or contain sensitive information please contact GovCERTUK for instructions.

CESG Enquiries
Room A2b
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Phone: 01242 709141
Fax: 01242 709193
E-mail: enquiries@cesg.gsi.gov.uk

Attachment D - Management and recovery plan of a reported incident

Incident

Classification - *What type of incident has occurred?*

- Loss of confidentiality of information
- Compromise of integrity of information
- Denial of Service
- Misuse of Service
- Damage to Systems

Priority and Urgency - *Identify the response level of effort for a given type of incident. These may be reordered to suit the Council's need:*

- Threats to the physical safety of human beings
- Root or system level attacks to any host or system
- Compromise of restricted confidential service accounts or software areas
- Denial of service attacks to infrastructure, confidential service accounts or software areas
- Any of the above at other sites which originate from the organization's systems
- Large scale attacks of any kind (worms, sniffing attacks, etc)
- Threats, harassment, or criminal offences involving individual user accounts
- Compromise of individual user accounts
- Compromise of desktop systems
- Forgery, misrepresentation, or misuse of resources
- Loss of removable media or portable equipment

Incident Handling Process

Contain the Incident - *Prevent problems with affected areas from spreading*

- Identify and isolate the area under investigation
- Notify law enforcement personnel and legal advisory if applicable
- Notify Public relations advisory if necessary
- Document containment information

Eradicate the Incident - *Put an end to whatever caused the incident*

- Gather evidence
- Identify the source of the incident
- Determine the full extent of the incident
- Implement stopgap measures to eliminate any active threats
- Update documentation with eradication information

Recovery Process and Follow-Up

Assess damages - *Determine the impact of the incident to the Council*

- Identify the affected systems and networks.
- Identify the affected data.
- Identify possible courses of remediation.

Reverse damages if possible - *Minimise the costs, both tangible and intangible, associated with the incident*

- Restore affected data from backup (if required)
- If necessary contact Communications with regard to press release.

Nullify the source of the incident - *Prevent recurrence of the same incident*

- Patch any open vulnerabilities (if technical issues)
- Improve access restrictions to the affected areas
- Further remediation as necessary

Review the Incident - *Learn from the mistakes*

- Determine why the incident was able to occur.
- Determine if the appropriate safeguards are in place to prevent recurrence.
- Determine the risk level of similar incidents to other information assets.

Review the Incident Handling Plan - *Adapt and increase efficiency in the response process.*

- Validate that the incident handling and response plan was appropriate.
- Modify the incident handling and response plan with new insight gained.

Documentation - *Keep tidy records, as they will almost certainly be needed again*

- Create final documentation of the incident in an appropriate level of detail.
- Perform debriefings if necessary.

Risk Registers – The need to review and/or amend Information Management, IT and Corporate Risk Registers.

- Review all necessary risk registers to ascertain if amendments are required.

Attachment E – GovCertUK Incident Reporting

GovCertUK Incident Report

General Information	
Reported By:	**Date/Time Detected:**
Department:	**Date/Time Reported:**
Title:	**Mobile:**
Phone:	**Fax:**
Email Address:	**Additional Information:**
Postal Address:	
Incident Details	
Type of Incident:	
Status of the Department (total failure, business as usual etc):	**Classification of affected System:**
Incident Details:	
Site Details:	**Site Point of Contact:**
Actions Taken:	

Appendix 6

Third Party Data Sharing Guidelines

Data sharing within the council

While service users might expect their data to be shared to give them the best service possible and whilst we want to encourage that for the effectiveness of the services, we can only do that if the user is aware that the data will be used in that way. A notice must be given at the time of collecting the data. The Legal law team should be consulted on the structure and format of that notice.

Data sharing outside the council (checklist)

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified? Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share? Key points to consider:

- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share it is good practice to have a **data sharing and/or confidentiality agreement** in place. As well as considering the key points above, your agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

One off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified? Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?

- Do you need to consider an exemption in the DPA to share?

Do you have the power to share? Key points to consider:

- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share, Key points to consider:

- What information do you need to share?
    - Only share what is necessary.
    - Distinguish fact from opinion.
- How should the information be shared?
    - Information must be shared securely.
    - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Appendix 7

Guidance and Procedure on Confidentiality

1. Introduction and Purpose

The purpose of this document is to provide staff with clear guidance and procedure in relation to the confidentiality of information and data.

All staff are bound by a legal duty of confidentiality. This means they are obliged to keep strictly confidential any person identifiable or commercially sensitive information that they may come into contact with whilst undertaking their council duties.

The Council is committed to the delivery of a first class confidential service. This means ensuring all personal information is obtained and processed fairly, lawfully and as transparently as possible so that staff/service users can:

- understand the reasons for providing complete and accurate information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the Council uses and handles information about them;
- understand their rights to access information held about them;

Staff should direct service users to the council's website (Information Charter) to obtain more details on how we handle their data securely.

2. Scope

For the purpose of this guidance/procedure, "staff" refers to permanent, fixed-term, contractors, agency, temporary, voluntary and students.

The requirement for confidentiality is:

- a legal requirement based on case law
- a requirement established in professional codes of conduct
- included within the Council's employment and other contracts and the Code of Conduct.

3. Accountability & Responsibility

3.1 The Head of Paid Services

The Head of Paid Services has overall accountability and responsibility for the management of the Council and ensuring appropriate mechanisms are in place for commissioning services. Maintaining confidentiality is essential to the Council being able to supply a first class confidential service that provides the highest quality to service users.

The organisation has a particular responsibility for ensuring that corporately it meets its legal responsibilities and for the adoption of internal and external governance requirements.

3.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Information Governance Lead with delegated authority from the Head of Paid Services. The SIRO provides assurances to the Head of Paid Services on the controls & procedures for managing information and chairs the council's Information Governance Board.

3.3 Caldicott Guardian

The Council's *Caldicott Guardian* has a responsibility for reflecting service user's interests regarding the use of Persons Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring that PID is shared in a lawful, appropriate and secure manner.

3.4 Information Governance Board

The Information Governance Board (IGB) will be represented by senior management to provide visible management support and clear direction for information security at the executive level.

3.5 All Staff

It is the responsibility of all staff to adhere to this guidance. Mandatory Information Security Training is provided via the council's main e-learning portal (Learning Pool). Staff should also regularly review this guidance and related policies/procedures to ensure they are aware of, and keep up-to-date with their individual responsibilities.

4. What is confidential (sensitive) information?

Confidential (sensitive) information can be anything that relates to service users, staff or any other information (such as confidential or commercially sensitive information contained in contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as service user's records, paper diaries, computer or on portable devices such as laptops, smartphones, mobile telephones) Persons Identifiable Information (PID) is anything that contains the means to identify a person.

A duty of confidence arises when one person discloses information to another (e.g. service user to staff in social care department) where it is expressly stated or it is reasonable to expect that the information will be held in confidence.

While service users might expect their data to be shared to give them the best service possible and whilst we want to encourage that for the effectiveness of the services, we can only do that if the user is aware that the data will be used in that way. A notice must be given at the time of collecting the data or as soon as possible afterwards. The Legal Team should be consulted on the structure and format of that notice.

Staff must ensure that the collection of any such data is fair and necessary, and that the recording and verifying of the information is accurate and consistent. Service users and staff must be informed of the importance of providing complete and accurate information.

5. Disclosing and using confidential (sensitive) information

It is extremely important that service users are made aware of information disclosures that must take place in order to provide them with highest quality of service. Similarly the need to share information between members of different teams and between different organisations involved in commissioning of services should be explained to service users. This is particularly important where disclosure extends to other organisations, especially where service users might not expect their personal information to be shared with those organisations.

Many uses of confidential/sensitive service user information do not contribute to, or support services that a user may receive. Very often these other uses are extremely important and may provide a more efficient and greater quality of service to a user. However, as they are not directly linked to the service requested, it cannot be assumed that a service user would be happy for their information to be used in this way and as such consent must be obtained.

Staff need to be aware that information disclosures of their personal information are also necessary at times to facilitate their employment. This may include, but is not limited to, disclosures to non local authority bodies, such as training providers and support companies.

6. Service user consent to disclosure

Service users have the right to object to the use and disclosure of their personal (sensitive) information and need to be aware of this right. Staff must therefore ensure that service users are made aware that the information they give may be recorded and shared, and the purposes for which this may apply (e.g. direct provision of housing etc.)

Staff should ensure that service users are informed of any information to be shared and whether they have any questions or concerns regarding this. If staff are unable to answer the questions or concerns, they must direct these concerns to their line manager. Advice and guidance can be sought from the Caldicott Guardian, SIRO, Service Manager – Information Management, Legal Services or other appropriate member of the Information Governance Board.

Staff should be able to explain the implications of disclosing or not disclosing information so that the service users can make valid choices. Sometimes this may mean that the service that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer other options.

7. Disclosing without consent

There are some circumstances where a decision to disclose without consent may be warranted. These include:

In the public interest / to protect the public: Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime, and / or to prevent abuse or serious harm to others. Definitions are not clear but examples include murder, rape, child protection concerns, fraud etc. There is an exemption in the Data Protection Act 1998 that allows the Council to give out personal information for these purposes (Section 29 – Crime and Taxation), but there are limits on what we can release. Whoever authorises the disclosure must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning used and the prevailing

circumstances. Disclosures should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies.

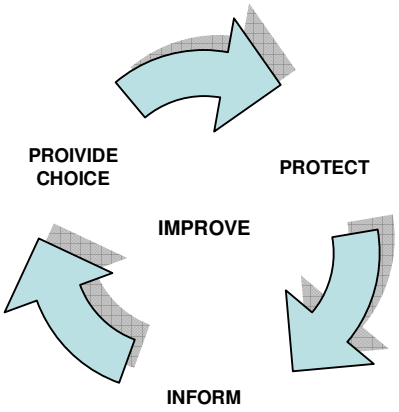
Where possible, the issue of disclosure should be discussed with the individual concerned and consent sought. Where consent is not given, the individual should be told of any decision to disclose against their wishes. This will not be possible in certain circumstances, for example where the likelihood of a violent response is significant, or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

Court order: A written request from the police that is backed by a court order, stating exactly what information is needed and its purpose. This does not require the consent of the service user but they should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with terms of the court order and to the bodies specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not relevant to the case in question, they may raise ethical concerns with the judge or presiding officer. However, if the order is not amended, a clear and accurate record of the circumstances should be kept.

Care should be taken in the method used to communicate such sensitive data to 3rd parties. All disclosures should be communicated in a secure manner and when sending emails of such a sensitive nature the use of GCSx, CJSM, Egress or other encrypted methods is mandatory.

8. The Confidentiality Model

The confidentiality model outlines the requirements that must be met in order to provide confidential service to service users/staff; they be must informed about the intended use of their information, give them the choice to give or withhold their consent, as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service.



The four main requirements are:

- **PROTECT** – look after the person identifiable information
- **INFORM** – ensure that they are aware of how their information is used
- **PROVIDE CHOICE** – allow service users/staff to decide whether their information can be disclosed or used in particular ways.
- I

  MPROVE – always look for better ways to protect, inform and provide choice

9. Legislation

Processing of PID is governed by the requirements of Acts of parliament and government guidelines. This guidance and procedure has been written to meet the requirements of:

- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act
- The Information Governance Toolkit
- Caldicott Guidance

10. Breaches of confidentiality

Staff may not access any personal information relating to relatives, friends or colleagues unless they have legitimate reason to do so as part of their employment responsibilities.

The Council proactively monitors the use of Information Assets including its IT Systems. Any ***actual or suspected breaches*** *of the Council' Acceptable Use Policy* will be dealt with under the Council's disciplinary Procedure.

11. Storage and destruction of confidential information

Confidential/sensitive information must be kept secure from unauthorised access or inadvertent alteration or erasure. Access and disclosure must be properly controlled.

It is vital confidential/sensitive information is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Please see the council's Information Governance and Security Policy for further details.

Appendix 8

Internal Information Sharing Protocol

Introduction

Harrow Council carries out a number of investigatory, regulatory and enforcement activities in relation to its statutory functions and takes legal action against people and businesses for a variety of purposes.

Harrow Council is a data controller under the Data Protection Act 1998 and is fully committed to complying with the requirements of the Data Protection Act 1998 (the "Act") in the way it collects and uses the personal information ("information") it holds.

Harrow Council holds information for the purposes specified in it's notification to the Information Commissioner, including the assessment and collection of tax and duties, the payment of benefits and the prevention and detection of fraud and crime, and we may use information for any of these purposes.

Where the law allows, Harrow Council will use information it has collected for one purpose for another lawful purpose. This is referred to as secondary use of information.

This protocol outlines the circumstances when investigatory, regulatory and enforcement departments will share information with, and obtain information from, other Council departments.

This protocol should also be used in conjunction with the Council confidentiality document which provides staff with clear guidance and procedure in relation to the confidentiality of information and data.

Purpose

This protocol is designed to:

- Govern the use and management of information held by Harrow Council investigation, regulatory and enforcement departments
- Support investigation, regulatory and enforcement action in accordance with relevant legislation (see below under Lawful Processing)
- Ensure compliance with the Data Protection Act
- Support the actions of Harrow Council in relation to the assessment and collection of tax and duties, the payment of benefits, the prevention and detection of fraud and crime and the prosecution of offenders

Information sharing

Information sharing refers to the exchange of information between one or more teams or service departments within Harrow Council. Advice from the Information Commissioner's Office is that local authorities may share information between different departments provided that they comply with the data protection principles set out in the Act.

The sharing of information may be necessary to identify, prevent and limit fraud and criminal activities and to prosecute offenders.

Information sharing will assist strategic and operational planning to prevent and detect fraud and crime, and will help Harrow Council to carry out its statutory functions in an efficient and effective way.

Benefits of information sharing

The benefits of appropriate information sharing are:

- Better informed decision making
- Better information management and recording
- Enhanced cross departmental working
- Improved detection and prevention of actual and potential fraud and criminal activity allowing
- More effective and efficient investigatory, regulatory and enforcement action
- Better targeting of resources
- Reduction of fraud and crime throughout Harrow Borough

Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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

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 those purposes.

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

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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.

Complying with the Data Protection Principles:

First Data Protection Principle – Lawful and Fair Processing

Lawful processing

Harrow Council must have a legal power to share or make secondary use of information for purposes other than those for which the information was given or obtained. This will usually mean being able to rely on an exemption from the non-disclosure and/or subject access provisions of the Act and being able to satisfy a fair and lawful processing condition under Schedule 2 of the Act (and also a Schedule 3 condition where the information is sensitive).

Although secondary use of information is not a disclosure of information to another under the Act it is useful to consider the most relevant potential exemptions from the non-disclosure and/or subject access provisions of the Act when deciding if it is fair and lawful to make secondary use of information within the Council. This is because the reason for making secondary use of the information within the Council will be relevant to assessing whether the secondary use is fair and lawful under the Act. The most relevant exemptions are:

- Section 29, which provides an exemption for personal information processed for

    - the prevention or detection of crime;
    - the capture or prosecution of offenders; and
    - the assessment or collection of tax or duty.

Where applying the non-disclosure and/or subject access provisions would be likely to prejudice any of those purposes, and

- Section 35 (2), which provides an exemption for personal information necessarily processed:

    - for or in connection with any legal proceedings (including prospective legal proceedings);
    - for obtaining legal advice; or
    - for establishing, exercising or defending legal rights

Fair processing

When collecting personal information from individuals in connection with its statutory functions, Harrow Council will ensure that where possible it will inform those individuals that it may share their personal information with other departments in specified circumstances (such as to assess and collect tax and to detect, prevent and prosecute fraud).

There are some situations when it will not be practical or possible to inform individuals about information sharing either because information sharing was not anticipated when the information was collected or because the information was obtained as part of an investigation. In these circumstances we need to rely on exemptions from non-disclosure of information contained in the Act set out above.

Second data protection principle

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

Unless a relevant exemption applies, Harrow Council should not obtain information for one purpose and use it for a completely separate and unrelated purpose. If the council is open and transparent about all the probable reasons for collecting information in the first instance and tells individuals that it may share their information with other departments at the Council then this will allow them to put that information to several uses in a variety of departments. In other situations, it will be important to check that one of the exemptions applies.

Third data protection principle

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

It is therefore necessary to ensure that only that information which is needed to achieve the specified purpose is shared with other departments.

Fourth data protection principle

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

If information is shared, a record should be kept to ensure that if information comes to light showing that data is not accurate, this can be passed on to other departments to ensure their data is kept up to date.

Fifth data protection principle

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

Each enforcement department will have their own policies on retention and destruction of information. It is important that data is properly destroyed when it is no longer needed.

Sixth data protection principle

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

Harrow Council has a duty to respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which it processes data and to comply with subject access requests in compliance with the Act, except where an exemption from the subject access provisions applies.

Seventh data protection principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All Harrow Council employees are bound by policies on data protection, information governance and acceptable use.

Eighth data protection principle

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of data protection.

As this protocol deals with sharing information within the Council, this principle is unlikely to be affected.

Checklist before Sharing Information:

1. Is it necessary for the department seeking the information to use the information to carry out its statutory function?

   In the absence of consent, the department would have to show why it is necessary to share the information e.g. failure to disclose would prejudice a crime prevention purpose.

2. If information is used for another purpose, what effect will this have on the people the information is about?

   This helps to identify whether sharing the information is proportionate. It is likely to be reasonable for Harrow Council to use its most up to date information to carry out its statutory functions and most individuals would expect that to be the case. Some particularly sensitive information, such as information about medical history or criminal conviction, should not be shared if there is any risk of unwarranted harm or detrimental treatment to the individual as a result of information being shared.

3. Would using the information cause unwarranted detriment to any individual?

   Detriment means harm, damage or distress. Personal data must only be used in a fair and responsible manner. Sharing information for the 'crime and taxation' and 'legal proceedings' purposes are unlikely to cause unwarranted detriment to anyone, even if it helps establish legal liability for tax or potentially fraudulent or criminal activity.

4. Would using the information for another purpose benefit those the local authority provides services to?

   This could include providing services based on more efficient use of public money and joining up enforcement functions in a way that saves money and so benefits local authority service users in a number of respects.

5. Is the information particularly sensitive?

   The sensitivity of information is not determined purely by its nature, but also by the context in which it is held. If information is linked to other data, it can become sensitive. Sensitive data such as information identifying a person's mental health should only be shared with other departments in order to protect the interests of that individual e.g. to assist an enforcement department to decide the most appropriate action, if any, to take against an individual.

6. Will the information be adequately protected from improper use or disclosure?

   Sharing information within the Council means that more people have access to the information and there may be a greater risk of it being misused. Harrow Council has clear policies on data protection, information governance and acceptable use which apply to all its employees and these are intended to ensure that information remains adequately protected from misuse or improper disclosure. The unlawful disclosure of personal information is a disciplinary offence and a criminal offence under the Act.

7. Is there an alternative to sharing information in a form that identifies individuals?

   In some cases, there will be no need to use information in a form that identifies people. Where possible, privacy enhancing techniques such as the anonymisation of information should be used to prevent the unnecessary use or disclosure of personal information.

8. Do individuals understand how the Council will use their information?

   Transparency will allow individuals to understand how their data is used and to complain if they object to this. Application forms requesting information should set out clearly how the Council intends to use a person's information. Other means should be used such as notices on relevant parts of the website. Also please refer service users to the Information Charter and the Fair Processing sections on our website.

Appendix 9

Third Party
Code of Connection

The council has a duty to safeguard the confidentiality and ensure the integrity of data pertaining to the citizens and businesses under its jurisdiction and other agencies with which it is in partnership, and make information systems available on an ongoing and timely basis.

The council has outsourced a number of systems management activities to Third Party specialist companies, and therefore the effective guardianship of data pertaining to citizens and businesses under its jurisdiction has become a responsibility of these Third Parties.

It is of paramount importance that every Third Party maintains the strength of security defined in the council's Information Governance & Security Policy. To this end, a Code of Connection is required between the council and any Third Party.

Traditionally, Service Level Agreements have focussed on availability of service. The Code of Connection addresses availability and the other two fundamentals of information security; confidentiality and integrity. The Code of Connection will be linked to, or included in the contract between the council and the Third Parties.

It is anticipated that third parties are aware of the information security requirements of local government organisations as specified by the government (for example in the electronic – Government Interoperability Framework (e-GIF) and Caldicott), and current legislation (Data Protection Act, Human Rights Act, Freedom of Information Act). The council also have a need to interconnect with other government organisations, such as the NHS, Police, Probation etc, all of which have minimum security level requirements and it is therefore essential that our connected partners also comply with these requirements.

The main areas that are considered in the code of connection include (but are not restricted to):

- Availability
- Business Continuity
- Incident reporting / management
- Integrity / confidentiality
- Logical Security
- Physical Security
- Data retention
- Data destruction
- Right to Audit
- Termination
- Data Protection
- Inter System File Transfer

The council will audit 3rd party suppliers security regime from time to time in order to verify that the security controls are appropriate. If deficiencies are identified, it will be the suppliers' responsibility and at its expense to carry out required corrective actions within specified timeframes.

Actions taken against Third Parties that do not comply with the Code of Connection may include suspension of service, removal from site, financial penalties, termination of any contracts and possible legal action.