Safe Information Handling Policy and Guidance

Version	Status	Date	Next Review Date
V3.0	Published	August 2021	August 2023

Contents

1 Policy Statement 2

2 Purpose and scope of this Policy 2

2.1 WHY THIS IS IMPORTANT 2
2.2 WHO THIS POLICY APPLIES TO 3
2.3 POLICY CONTEXT 4

3 Information Security - the County Council's obligations 4

4 Principles of safe information handling 5

4.1 MAINTAINING COUNTY COUNCIL BUILDINGS AS 'INFORMATION SAFE HAVENS' 5
4.2 MAINTAINING INFORMATION SECURITY WHEN WORKING FROM HOME 5
4.3 KEEPING INFORMATION SECURE IN COUNTY COUNCIL SYSTEMS 5
4.4 THE LEVEL OF SENSITIVITY OF INFORMATION DETERMINES ITS HANDLING 6
4.5 DECIDING ON THE LEVEL OF SENSITIVITY OF INFORMATION 6
4.6 CHOOSE THE CORRECT WORKING PRACTICES BASED ON THE SENSITIVITY LEVEL OF THE INFORMATION 9

5 Safe in our Hands 10

6 Information Sharing 11

7 Social Media 12

8 What to do if information may have been lost or compromised 12

9 Office Moves 12

10 Information handling roles and responsibilities 13

10.1 RESPONSIBILITIES OF ALL STAFF 13
10.2 LINE MANAGER RESPONSIBILITIES 13
10.3 SPECIALIST ROLES AND RESPONSIBILITIES 13

11 Appendix 1: Levels of sensitivity of Council information 14

12 Appendix 2: Secure information handling standards 15

1 Policy Statement

Hampshire County Council has a duty under the principles of the UK General Data Protection Regulation (UK GDPR) to ensure that the personal data it processes, stores, and uses is kept safe and secure, and protected from loss, destruction, or unauthorised disclosure.

The County Council has a legal and moral obligation to individuals to safeguard their personal and/or special category data.

Guidance to ensure compliance with the UK GDPR and Data Protection Act 2018 (DPA) is also contained in the Data Protection Policy and Data Protection (GDPR) eLearning package on the LMS. Information about other Data Protection issues can be found on the Data Protection intranet pages. Further details on IT security are provided in the Corporate Acceptable Use, Remote Access Use, and Security Incident Reporting Policies and on the IT Security intranet pages.

This Policy applies to anyone who handles personal and/or special category data on behalf of the County Council, such as employees (including employees who are working out their notice period, and seconded employees), workers, contractors, volunteers, interns, apprentices. Throughout this Policy, this group will be referred to as “staff”). The information handled might be paper-based, electronic or in any other format including spoken information.

Staff are expected to **use their judgement** when determining the level of sensitivity of particular information and to take appropriate action to protect information, taking the guidance within this Policy into consideration.

Information created and held for the purposes of the County Council for its services or business is the intellectual property of the County Council regardless of where it is stored.

It is the responsibility of all staff handling personal, special category and high-risk business information to be able to **demonstrate that they have followed the policy and standards**.

In the event of a potential data protection incident taking place, involved individuals will be asked to **show that they took the precautions set out in the policy and standards**. If they took a different approach, they will be asked to **show how this was in keeping with the principles of this policy and the associated standards**.

2 Purpose and scope of this Policy

2.1 Why this is important

The aim of this Safe Information Handling Policy is to promote good working practices , and enable and support staff in how they handle information.

The impact of poor information security practices can have a significant effect on the lives of those customers and clients who we hold information on, many of whom are the most vulnerable in the community. It can also have reputational, financial, and commercial consequences for the County Council.

We all have a responsibility to respect our customers and ensure that the information we hold on them remains ‘safe in our hands’. We also need to protect high risk business information.

The safe working practices set out in this policy and its accompanying standards will help to ensure that staff keep information within ‘information safe havens’, i.e. safe environments and safe working practices which help to protect it from unauthorised disclosure.

Safe information practices are especially important as they help to safeguard information when it is vulnerable, e.g. when it is taken out of the office or conveyed to third parties, whether by post, email, fax, the spoken word or any other means.

The safe information practices also apply to information held within the County Council. We have a responsibility to ensure that only authorised staff access personal information and that it is only used for the purpose for which it was collected.

Where personal and/or special category information is being handled or transferred in circumstances which fall outside the 'information safe haven' locations and practices described in the policy and standards, staff must think carefully about whether the action is necessary and, if so, how information security can be ensured.

This Policy outlines the practical steps for keeping all sensitive information safe. This primarily means personal and special category information about our clients, customers and staff, but also includes information that is High Risk Business Information.

For the purposes of this Policy "Sensitive Information" refers to personal and special category information as defined by the UK GDPR and DPA together with other sensitive information as defined by the County Council, such as Business Sensitive Information, as outlined in 4.3 below.

More information can be found on the Data Protection pages and in the mandatory Data Protection eLearning (search for "Data Protection (GDPR)" under "Find Learning").

2.2 Who this Policy applies to

This Policy applies to anyone who handles Sensitive Information on behalf of the County Council, whether this is paper based, electronic or in any other formats including spoken information.

It sets the standards by which the County Council expects that its information should be treated and therefore applies to any other person who has responsibility for, or is required to access, process or transmit, data obtained and stored by or on behalf of the County Council, e.g. agency workers, contractors, volunteers etc.

Staff are personally responsible at all times for the information, in whatever format, in their care. They must safeguard the security of personal and special category and high-risk business information for which they are responsible or which they access in order to carry out their work and conform with the data protection Principles, only using information that they need to complete the tasks associated with their role.

Security access to systems that hold personal information will be tailored so that staff have access to the information they need to undertake their roles. However, in some cases management controls will be in place whereby although staff may physically be able to access certain personal information, they are not authorised to access and so should refrain from doing so. Staff will be informed of the systems they are authorised to access and the extent of their authorised use.

When handling information when using any IT systems or equipment for work, staff must also adhere to the standards contained in the Corporate Acceptable Use Policy (see the IT Policies and Security page). This defines misuse and other significant policy areas. Further examples of acceptable use and misuse are set out in a guidance document which should be read in conjunction with the Corporate Acceptable Use Policy, and can be found within the Policy on the IT Policies and Security page.

Inappropriate or unauthorised access to personal information would constitute a failure to meet the standards outlined within this Safe Information Handling Policy.

The County Council will enforce this Policy through its Managing Misconduct Policy. Breaches of this Policy could lead to disciplinary action and penalties up to and including dismissal, depending on the breach and its impact on the County Council.

As stated in the County Council's Data Protection Policy for Staff, examples of misuse or unacceptable behaviour include:

1. Inappropriately or without authorisation, removing personal, special category, sensitive, confidential or high-risk business information from the organisation's premises, IT systems or environment where it is usually stored;
2. Loss or inappropriate sharing or dissemination of personal, special category, sensitive, confidential or high-risk business information from the organisation's premises, IT systems or environment in which it is usually stored;
3. Inappropriately or without authorisation, accessing personal, special category, sensitive, confidential or high-risk business information that they are not entitled to for the purposes of their role;
4. Failing to report a possible/potential data protection breach or failing to assist with the investigation into such a data breach;
5. Through action or inaction allowing, permitting or causing staff under their control to operate in such a manner as any of the above occurs.

Staff should be aware that it may be a criminal offence to knowingly or recklessly obtain, disclose, procure, or retain the disclosure of personal data without the consent of the County Council.

2.3 Policy context

This Safe Information Handling Policy should be read in conjunction with other relevant County Council policies, particularly the County Council's Corporate Acceptable Use Policy, Data Protection Policy for Staff, SharePoint Security documents, Code of Conduct, General Privacy Notice, IT security using guides, Policy for dealing with Potential Data Protection Incidents, Social Media Policy and the County Council's Data Protection Policy.

3 Information Security - the County Council's obligations

The County Council has a legal and moral obligation to its service users, citizens, staff, partners and other stakeholders to safeguard personal and special category information it processes, stores, and uses. It is obliged, under the terms of the UK GDPR and DPA to ensure that all personal and special category information is secure and protected from unauthorised or unlawful use, loss, destruction or damage.

There are two areas which staff are personally responsible for at all times:

	Information about People
	This includes:
a)	Personal information i.e. can be linked to and/or identifies customers, service users or staff and tells you something about that person (different levels of sensitivity are discussed later in 4.3 of this document).
b)	Special category information i.e. information which reveals sensitive information about an individual, such as health information or religious / political opinions.
c)	Information which is restricted or confidential at law i.e. an actionable breach of confidence. This is when information was provided to us in confidence and if the County Council disclosed information the provider or third party could take the County Council to court.

Information about the Business: High Risk Business Information
This includes: a) Information which, if not protected, could expose the County Council to fraud, i.e. financial codes, or individuals' signatures. b) Confidential business or commercial information, i.e. confidential committee reports, tenders or contracts information that relate to a contractual agreement between the County Council and a supplier/other organisation. c) Information, which if not protected could impede the County Council's regulatory or other statutory responsibilities i.e. some civil or criminal investigations.

4 Principles of safe information handling

4.1 Maintaining County Council buildings as 'information safe havens'

To help to protect the information held in the 'information safe haven' location of County Council offices, all staff are responsible for supporting office security. They should:

- not allow unauthorised people into areas where Sensitive Information is kept unless supervised,
- not allow tailgating at entrances,
- ask to see the ID of individuals entering a building at the same time as them without independently using their swipe card,
- always wear ID cards visibly (minimising the need to challenge staff at entry points),
- exercise discretion before discussing personal / special category information in public areas, including public transport, café areas and Drop-In centres, and
- not display or store sensitive information in a way that could be visible from outside of a secure area, such as keeping records on a windowsill on the ground floor.

4.2 Maintaining information security when working from home

When working from home, all staff need to maintain the security of the information that they use. They should:

- Set up a suitable work area where you can minimise your screen being visible to others, and lock your screen (Windows key + L) when you step away from your desk
- Use a headset to maintain confidentiality of conversations
- Keep paperwork and devices locked away or, if not possible, out of sight of other people at home when not in use, and
- Report any concerns to your manager as soon as possible

Detailed information can be found on the Data Protection intranet pages.

4.3 Keeping information secure in County Council systems

Staff must comply with the Corporate Acceptable Use Policy. They should:

- only use approved technology for handling County Council information,
- keep their passwords secure and not share them with others,
- not open suspicious attachments,
- report potential phishing emails,
- lock documents and records down with the appropriate levels of security so that only authorised staff can view personal details, and
- never include personal or special category information in meeting requests or attach documents to Outlook Calendar appointments that include personal details.

4.4 The level of sensitivity of information determines its handling

The County Council is responsible for a diverse set of information, from information that is in the public domain to highly sensitive personal information.

To manage information appropriately, staff must first identify the level of sensitivity of information and use this as the basis to confirm suitably secure working practices. In general, the more sensitive the information being handled, the more care should be taken processing, storing, or using that information.

4.5 Deciding on the level of sensitivity of information

Staff are expected to **use their judgement** when determining the level of sensitivity of particular information, taking the guidance within this Policy into consideration.

Information about People
The personal information handled by the County Council about individuals can be classified into two broad levels: **high risk sensitive (special category) data** and **personal data**. They essentially relate to levels of privacy.

Examples of Sensitive Data:

Special Category Data High Risk Sensitive (HIGH RISK)	This includes data defined by UK GDPR as Special Category Data, data defined by the DPA as having a similar status, and data defined by the County Council as high risk. Information revealing an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Health data • Sex life or sexual orientation • Genetic Data or Biometric Data • Criminal offences and proceedings (committed or alleged) E.g. medical records, core assessments, Adults' Health and Care Assessments, SEN Statements, Care records, Occupational Health records, fingerprints. The circumstances of the individual's life are relevant to determining whether straightforward personal information (name, address etc.) should be viewed as High Risk Sensitive Data. Additional information viewed as sensitive and high risk by the County Council: • National Insurance number • Financial/payroll details • HR records
Personal Data (MEDIUM RISK)	Personal data is any information that relates to an identified or identifiable living person. This can include (but is not restricted to): • Name • Address • Date of birth • Telephone number • Email address • Location data • Online identifiers • Identification numbers Information found in the public domain that identifies somebody is still personal data. (Remember, the circumstances of the individual's life might mean that this information should be handled as High Risk Sensitive Data, e.g. domestic abuse/safeguarding).

Staff should also consider whether the context or volume of medium risk data is such that it should be treated as high risk. For example, considering additional security measures when sending or

transporting large volumes of lists of names/other personal data. Some personal data may also need to be handled as high risk because of its context, for example domestic/abuse/safeguarding.

Staff should familiarise themselves with these levels of sensitivity so that they are able to categorise the information they are handling. More examples are included in Appendix 1.

Staff must also undertake the Data Protection eLearning module (called "Data Protection (GDPR)") as part of their induction and at regular intervals as required. This eLearning contains further training and guidance regarding UK GDPR, the sensitivity of different types of data and the obligations set out in the legislation. More information can be found on the Data Protection intranet pages. There may also be additional training requirements depending on your department and role.

High-Risk Business Information

As well as information about people, the County Council also holds information that relates to its business operations where it needs to control the distribution of that information. Often this means restricting access to other parties, i.e. outside the County Council, or even within the organisation itself.

We have defined this as 'High-Risk Business Information' and it includes information relating to trading or commercial activities undertaken by the organisation; information relating to the formulation of County Council Policy, including items restricted under Schedule 12A of the Local Government Act 1972. Information of this kind, that requires a high level of confidentiality, should be treated in the same way as special category data.

As with defining the sensitivity of personal information, staff should **use their best judgement** to determine the appropriate level of confidentiality.

An example of the County Council's approach to confidential information is its use of Schedule 12A to restrict the publication and distribution of confidential reports to Elected Members.

High Risk Business Information	Examples that could be considered: • Information relating to the financial or business affairs of the County Council, including contemplated, as well as past or current, activities e.g. trading activities. • Information relating to any consultations or negotiations, or contemplated consultations or negotiations, in connection with any labour relations matter arising between the County Council and its staff. • Information relating to any action taken or to be taken in connection with the prevention, investigation or prosecution of crime. • Legally privileged information. • Information provided to the County Council where it is bound by the law of confidentiality. • Information where distribution is restricted by Government regulation, legislation or court order.

Depending on the reasons for confidentiality, high-risk business information might only be confidential for a limited period of time.

It should be remembered that defining a set of information as 'high-risk business information' does not automatically exempt that information from disclosure under the Freedom of Information Act 2000. Careful consideration would need to be undertaken under the terms of that Act, including relevant exemptions and, where necessary, the public interest test.

Low Risk Information

All other information held by the County Council (i.e. information that doesn't fit the above Medium and High Risk criteria) can be considered as Low Risk.

This should still be handled with care and consideration but requires fewer precautions.

4.6 Choose the correct working practices based on the sensitivity level of the information

For guidance on how this should be done, *Appendix 2: Secure information handling standards* presents a set of information handling standards in tabular form. It explains how to store, use, transmit and dispose of information in different formats and at the different levels of sensitivity.

Staff should use the table to check the appropriateness of their current information handling practices and procedures and to decide how to proceed when faced with any new information handling scenario.

The standards cover:

Paperwork

- Secure management of paperwork in the office, outside the office and at home.
- Secure disposal of paperwork.
- Secure printing, copying and scanning.
- Secure posting practices, both internally and externally.
- Hand delivery of documents.
- Secure faxing (outgoing and incoming).

Electronic information

- Secure storage of electronic data.
- Preventing inappropriate access to electronic information.
- Destruction of electronic information.
- Secure emailing and other methods of electronic communication.
- Choosing appropriate tools for sending information to third parties.
- Choosing how to send sensitive information to service users.
- Secure use of shared Outlook diaries.

Verbal information

- Secure telephone use in and outside the office.
- Secure handling of incoming calls.
- Meetings or discussions in places where speech may be overheard e.g. Council coffee shops, public places

Recordings

- Meetings with service users/clients
- Internal meetings
- Meetings with external organisations
- Live events

These standards are informed by:

- the UK GDPR (see below in 3.4.7), the DPA and guidance from the Information Commissioner's Office (ICO) on appropriately secure practices helping data controllers to meet these principles, and
- the **Caldicott Principles for protecting personal and/or special category information.** These principles originated in the health and social care sector but provide valuable guidance for any handling of personal and/or sensitive information.

It is the responsibility of all staff handling personal and/or special category information to be able to **demonstrate that they have followed the policy and standards**.

The policy and standards cannot cover every eventuality. Therefore, **'equivalent approaches or practices' may sometimes be appropriate**, informed by the Principles in the UK GDPR.

If you are in doubt about the appropriateness of your approach, contact the County Council's Information Governance Team (data.protection@hants.gov.uk) for advice.

In the event of an information security incident taking place, involved individuals will be asked to **show that they took the precautions set out in the policy and standards**. If they took a different approach, they will be asked to **show how this was in keeping with the principles of this policy and the associated standards**.

UK GDPR – the Principles Relating to Processing of Personal Data

Personal data shall be:

(a) **processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');
(b) **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
(c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');
(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) **storage limitation**; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
(f) **processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5 Safe in our Hands

The County Council must put the rights of the individual at the centre of everything we do with their data. Individuals have a number of rights under the UK GDPR, including;

- The right to be informed
- The right to erasure (also known as "the right to be forgotten")
- The right of access (also known as a "subject access request")

Further information is available on Hantsweb and on the Data Protection pages.

We must be transparent in the way we process their information, ensuring that we comply with the Principles of the UK GDPR. Wherever personal or special category data is being processed, a Privacy Notice must be provided.

Personal and special category data can only be processed if there is an appropriate lawful basis taken from the UK GDPR for processing. That basis must be set out in the Privacy Notice. Guidance on the potential lawful bases for processing can be found on the Data Protection pages.

Projects that use personal and special category data must be assessed for potential data protection risks. This is achieved by completing a Data Protection Impact Assessment (DPIA). A DPIA helps identify any potentially high-risk processing, which could infringe on individual's rights.

Further information on drafting a Privacy Notice and undertaking a DPIA can be found on the Data Protection pages.

Any records held by the County Council should be kept in compliance with the relevant retention schedule.

Any use of personal and special category data must be recorded by the County Council as part of its Data Flow Mapping and Record of Processing Activities (ROPA). This helps processing remain transparent and keeps all vital information about processing together. Departmental Data Protection Co-Ordinators will hold each department's ROPA.

6 Information Sharing

Before sharing information, checks should be made to ensure the County Council has a 'lawful basis for sharing'.

To comply with UK GDPR and other relevant legislation, before sharing personal and/or special category information with third parties, staff need to ensure not only how to protect the security of information being shared but also:

- whether the County Council has a lawful basis to share the information, and that only the relevant information is shared, and
- whether that sharing is justified e.g. by a lawful basis under the UK GDPR such as the data subject's consent.
- where personal and/or special category information is being shared on a regular basis between organisations working together in a partnership, a data sharing agreement must be in place. All data sharing agreements must be added to the Data Sharing Register, which are held by Departmental Data Protection Coordinators.
- where there is a contract in place with a supplier, this is not data sharing. Appropriate data protection clauses will need to be included. Please seek Legal advice.

The reason for sharing and the lawful basis for sharing needs to be confirmed during the process of drawing up the agreement or contract. Enquiries should be made to ensure that all involved organisations can meet each other's security and information management requirements.

The existence of a data sharing agreement or a lawful basis for sharing does not entitle an organisation to share personal or special category information. A lawful basis under the UK GDPR must always be included. Seek further advice where necessary.

The County Council has a number of existing information sharing agreements in place which provide guidelines on sharing specific information with particular partners.

A Data Protection Impact Assessment may also be required.

Prior to information being shared, the questions of whether the sharing is justified and whether the County Council has a lawful basis to share must be addressed. If in doubt about whether to share information, staff should consult their line manager, contact their **Departmental Data Protection Co-ordinator** or contact the Information Governance Team (data.protection@hants.gov.uk) for advice.

Before sending special category information or a large volume of personal data to third parties, staff must also consider whether the information will be transmitted securely and securely managed when it reaches its destination. This must be addressed by the agreement and/or the contract before the information is sent.

7 Social Media

When using any social networking platform staff should comply with the County Council's Social Media Policy. This aims to ensure that staff can play an active part on social media, while complying with the relevant corporate policies, and with legislation. The policy covers professional use for business purposes, and also sets out expectations around staff personal use of social media where personal use could have an adverse impact on their role, or on the County Council's business or reputation. Individuals should ensure they are aware of their obligations and responsibilities and adhere to this policy.

If you are intending to use social media to gather personal or special category information about people to inform decisions made by the County Council, you will need to make your line manager aware that you intend to undertake this task and confirm, and you will need to speak to your Departmental Data Protection Coordinator regarding the lawful basis, and whether this activity is necessary and proportionate. Be aware that social media surveillance could be classed as unlawful if it interfered with an individual's right to respect for private and family life, home and correspondence.

Accompanying the Social Media Policy is a Social Media Guidance document for staff and managers, with some frequently asked questions about social media in the workplace.

8 What to do if information may have been lost or compromised

Staff should follow the steps outlined in the Policy for dealing with Potential Data Protection Incidents, which can be found here:

In the event of discovering that personal information has potentially been mislaid, taken, sent to the wrong person, or shared inappropriately, staff should:

Step 1: Immediately contact their line manager or key Council contact.

Step 2: Take steps to retrieve the information, including:

- Attempting to recall an email sent to the wrong person(s) internally
- Asking the recipient to delete the email from their inbox and deleted items
- Contacting the recipient of wrongly disclosed information and asking them to return the information, or collecting the information yourself
- Retracing your steps or searching the immediate area for mislaid paper documents.

Step 3: Make sure the County Council's Information Governance Team is informed **as soon as possible** using the Reporting a Data Incident Form. This is sent to data.protection@hants.gov.uk and the Departmental Data Protection Co-ordinator will be informed.

A **Reporting a Data Incident Form must be completed, please provide as much information that you have at that time, but do not delay in submitting it even if you do not have all of the information.**

Step 4: Also contact the IT Service Desk on 01962 847000 if this relates to an IT system or device.

Step 5: The County Council will then implement the procedures for investigating and assessing the incident outlined further in this document.

9 Office Moves

When moving workplaces, staff must initiate the Office Moves procedure. Each department has an Office Moves Coordinator who provides advice and practical support when office moves are being

undertaken. By following this procedure, potential data incidents can be avoided, and information will be processed safely.

10 Information handling roles and responsibilities

10.1 Responsibilities of all staff

Staff are personally responsible at all times for the information, in whatever format, in their care. They must safeguard the security of Sensitive Information for which they are responsible or which they access in order to carry out their work.

It is the responsibility of all staff to familiarise themselves with this policy prior to handling information or sharing it with third parties, and to use the policy and standards to inform their information handling choices. Staff should seek advice from their line manager, Departmental Data Protection Coordinatorv, or Information Governance Team if they are in doubt about how to apply this policy.

Staff should contact their manager or use the County Council's Whistleblowing Procedure to report any concerns about improper use of County Council information or practices likely to result in an data protection or information security breach.

10.2 Line manager responsibilities

Line managers have a responsibility to ensure that all staff are instructed in their responsibilities in relation to working with personal and special category and high-risk business information. Line managers should satisfy themselves that staff reporting to them are aware of and comply with relevant data protection, information security and IT policies (*Appendix 4: Associated policies and guidance*).

Line Managers are to ensure that all staff have completed the appropriate Corporate and departmental Data Protection training.

Managers should be alert to any potential breaches of this policy that could lead to a data protection or information security incident and seek advice from Information Governance and/or take appropriate preventative action. Managers must investigate and take relevant action to address information security incidents in accordance with the Policy for dealing with Potential Data Protection Incidents, found here.

10.3 Specialist roles and responsibilities

Information about the responsibilities of officers within the Information Governance structure can be found here.

11 Appendix 1: Levels of sensitivity of Council information

This table provides detail on the type of information covered by different levels of sensitivity and gives examples of each.

Sensitivity level	Impact level if information was lost or compromised	Examples
LOW RISK	• Little or no impact on the finances of the County Council. • No inconvenience or distress to the individual. • Little or no financial impact to the individual. • Little or no impact on the County Council's standing or reputation.	• Policies and procedures. • Documents available in the public domain e.g. via the County Council website. • Names and contact details of staff that are in the public domain or where the individual has authorised this. • Many performance statistics.
MEDIUM RISK Including Personal Data	• Short-term inconvenience, harm or distress to an individual. • Financial loss or loss of earning potential. • Facilitates improper gain. • Breaches statutory restrictions on the disclosure of information • (e.g. under the UK GDPR / DPA). • Damage to the County Council's reputation. • Financial impact to the County Council. • Undermines the confidentiality of information provided by individuals or third parties.	• Personal information relating to any service user or employee for which we have a duty of care such as name, address, contact details • Documents from an employee record or service user case file IF THEY DO NOT contain the level of information covered by the heading below. • Exempt committee papers or discussion documents excluded from the public. • Draft documents before approval for release into the public domain.
HIGH RISK Including Special Category Data and High Risk Business Information	• Substantial inconvenience, harm or distress to any number of individuals. • Short-term inconvenience, harm or distress to a large number of individuals. • Causes greater financial loss or loss of earnings potential. • Facilitates greater improper gain or advantage. • Substantial damage to the County Council's reputation. • Significant financial impact to the County Council (£1m +). • Prejudices the investigation of or facilitates the commission of low-level crime, hinders detection of serious crime. • Includes information relating to trading or commercial activities undertaken by the County Council; • relating to the formulation of Council Policy, including items restricted under Section 12A of the Local Government Act 1972.	• Employee records or service user case files which contain information about: • Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sexual life or sexual orientation, genetic data or biometric data or criminal offences and proceedings (committed or alleged). • National Insurance number, IDs from which the identity of individuals can be looked up and signatures. • **Large amounts of personal data**, so that the loss would affect a large set of people (e.g. over 100). • Investigation files.

12 Appendix 2: Secure information handling standards

First identify the sensitivity level of your information then use the table to confirm appropriate working methods to protect its security. If in doubt, contact data.protection@hants.gov.uk

A2.1 Secure handling of paper-based information

Handling paperwork			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Including Special Category Data and High Risk Business Information).**
Handling paperwork in the office	Maintain a clear desk at the end of the day, in line with the Clear Desk Policy.	Remove documents from your desk at the end of the day. When not in use, store paper based personal information in locked drawers/cabinets. Prevent casual viewing of information in use. When you leave your desk, documents can be left face down on the desk for short periods as long as you are still in and around the office.	As for Medium Risk plus Do not leave unsupervised on desks or in unlocked cupboards. If appropriate, place lockable cabinets in a part of the office where access can be restricted.
Handling paperwork outside the office	Take reasonable precautions to look after information.	Hold information under lock and key when not in use, e.g. in a locked bag. If possible, store sensitive documents separately from IT equipment. When using your car to transport information, keep documents and devices out of sight, and do not leave these in your car overnight. Consider implementing a ‘booked out’ filing system where a record is kept of what is taken or sent, by whom and to where, and record when it is returned.	As for Medium Risk plus Case workers should make a log of case files that have left the office (e.g. to support home visits etc.) and when they are returned.

Paperwork at home	Take reasonable precautions to look after information in the same way as in the office.	Take home the minimum amount of paperwork necessary and keep it there for the minimum time required. Consider how you could work electronically to avoid using hardcopy documents. Keep paperwork and devices locked away or, if not possible, out of sight of other people at home when not in use. Avoid keeping paperwork in laptop bags in case of burglary. Do not dispose of or shred paperwork at home. Return it to the office for secure disposal.	As for Medium Risk
Secure disposal of paperwork	Use recycling bins for paper.	Deposit in confidential waste bins for secure shredding. Never put it directly into a general waste bin or recycling bin.	As for Medium Risk plus Consider ripping up or shredding paper prior to depositing it in the confidential waste bins for additional security.
Vacating office premises (permanent move)	Remove all files to new location SEE Office Moves procedure	Arrange for client/personnel files to be securely transferred to new location. Dispose of any paperwork that is not required in confidential waste bins. Arrange for files that are no longer needed but must be retained under the Retention Schedule to be collected or sent securely to the Records Management team with responsibility for your department.	As for Medium Risk plus Do not leave paperwork in any building that is being vacated either temporally or permanently. Check that all cupboards and filing cabinets in your areas are clear (empty). Check that FM are aware that there are confidential waste bins to be collected.

SECURE PRINTING, COPYING AND SCANNING			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Including Special Category Data and High Risk Business Information.**
Secure printing	Collect printouts from printers or MFDs promptly.	Always use secure printing processes. Collect all documents promptly from the printer. Personal information must be collected immediately, not left where anyone can see it. On Printsmart printers once you have pressed 'Print', you are releasing documents to the device. It is your responsibility to ensure that the printing of the documents is completed. If the device runs out of paper or jams, the documents will be held on the printer and printed once the jam is cleared or tray filled so make sure all your documents have been printed or cancelled before you leave the printer. There is advice on how to cancel print jobs on laminated paper in resource areas. Following these instructions will allow you to see if all printing has been completed and will show how to cancel any jobs that have been sent to print.	As for Medium Risk plus
Secure scanning	Collect documents promptly.	Do not leave the MFD during scanning.	As for Medium Risk

SECURE USE OF POSTAL SERVICES			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Including Special Category Data and High Risk Business Information)**
Preparing documents to post		To avoid mistakes when sending out personal information: • Prepare mail for one recipient at a time wherever possible and do not prepare sensitive letters in a hurry. • Before sealing the envelope, double check that the **letter** and **all the pages of the attachments** are for the intended recipient. • Take particular care when preparing mail merge documents. Only send out the minimum amount of personal information necessary. Follow the Principles Relating to Processing of Personal Data (above). Check the name and address is correct.	As for Medium Risk plus For an extra level of assurance, ask a colleague to double check that all the contents of an envelope are the correct ones for the intended recipient.
Sending paperwork via County Council internal mail	Follow courier instructions. All mail MUST be clearly addressed – this must consist of a name, HC Collar Number where appropriate, destination location and Courier Code. All mail must be in envelopes or plastic mail pouches. If this is not possible please ensure that is securely bundled with elastic bands or string. All mail must be clearly labelled with the destination address and Courier Code. SEE Guide to sending out mail within HCC buildings	Place in a sealed envelope marked “Confidential”. Address to an individual by name or job title. Please be aware that there are additional precautions you should take to ensure secure delivery when sending medium or high-risk information via internal couriers. Please see process outlined on courier service page on Hantsnet. This includes an option to have internal mail tracked. Courier confidential mail instructions	Place in a sealed envelope marked “Confidential”. Contact the recipient before sending to: • check their address in case they have recently moved office. • check they will be available to receive it. Address to an individual by name or job title. Include the box number for their office. Consider tamper proof envelopes or hand delivery.

Sending paperwork via the Post	Ordinary envelope through public mail system	The address should be typed and be clearly visible through the envelope's window if it has one. Include a return address on the letter or package so that it can be returned without being opened if undelivered or if sent to the wrong address. Mark 'Addressee only' or 'Private and Confidential'. Consider tamper proof envelopes. If – exceptionally – you are sending electronic data by post (USB stick, CD, etc.), the content of that electronic data **must** be encrypted.	Avoid sending this type of information by post. Wherever possible, use secure electronic options e.g. encryption. Consider using Special Delivery. This tracks the item during transit and requires a signature on delivery. SEE Sending recorded or special delivery mail The address should be typed and be clearly visible through the envelope's window, if it has one. Include return address on the letter or package so that it can be returned without being opened if undelivered or sent to wrong address. Use appropriate stationery, e.g. tamper proof envelopes, reinforced where necessary. Consider double bagging the package, including details of the sender and recipient on both layers. You should not post electronic information at this level of sensitivity, e.g. on a USB stick or CD. More secure electronic alternatives are available, namely encrypted email.
Hand delivery/collection of documents outside of the Council	Not usually necessary but may be considered depending on the customer's needs. Wear your work ID badge to prove your identity. Arrange a suitable time with the customer. Package documents to allow these to be posted through the letterbox or left in a designated safe space.	As for Low Risk, plus: If there is a large volume of personal data, the safe space is unlikely to be a suitable drop-off point unless it is lockable. Include a return address on the packaging in case the items are misplaced. If the delivery is unsuccessful, return the documents to the office and store these securely.	As for Medium Risk, plus: Consider using tamper-proof envelopes when packaging documents. Delivering to a safe space will not be suitable unless it is lockable.

SECURE FAXING			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Including Special Category Data and High Risk Business Information)**
Deciding whether to fax a document	Ok to use a fax, but likely to be more efficient to communicate electronically.	**Faxing should generally be avoided as it is insecure.** Fax machines must only be used to transfer personal information where it is absolutely necessary to do so and there is no more secure alternative, e.g. secure email Seek advice from your line manager or the Information Governance Team if you are unsure whether or not to send sensitive information via fax.	As for Medium Risk
Safe management of incoming faxes	Pick faxes up promptly.	If a fax machine is needed, site it in an appropriately restricted area. A responsible person must ensure that the fax machine is working and has sufficient paper loaded so that incoming faxes are received as soon as practicable. Faxes containing sensitive information must be picked up straightaway and receipt confirmed with the sender. If sensitive material is left at the fax machine, notify your Data Protection Coordinator or if they are not available, the Information Governance Team. Fax machines should be turned off out of hours to avoid sensitive material sitting for an extended period on the in-tray.	As for Medium Risk

Safe sending of faxes	Normal use of a fax machine	Include a fax header page, indicating the sensitivity level of the information. Only send the minimum necessary personal information and anonymise information where possible. Check the fax number before dialling, and then take care in dialling the number. Programme frequently used numbers into the fax machine 'memory dial' facility to minimise the risk of dialling incorrect numbers. Double check these numbers have been programmed correctly. Ideally, faxes should be sent to a safe location where only staff who have a legitimate right to view the information can access it. If this is not the case or not known, take extra precautions: • Notify the recipient that a fax will be sent to ensure that they are available to receive it. • Obtain confirmation of successful transmission and attach this to the original document. • Ask the recipient to confirm safe receipt.	As for Medium Risk Only use faxes when there is no alternative

A2.2 Handling electronic information

STORAGE, ACCESS AND DISPOSAL			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Including Special Category Data and High Risk Business Information)**
Storing electronic data	Follow the Corporate Acceptable Use and Mobile Device Policies.	Store information securely and where using SharePoint ensure the permissions levels are appropriate. In line with the Mobile Device Policy : • Store the minimum information on mobile devices and for the minimum period of time necessary. • Ensure mobile devices, including laptops and USB sticks, are encrypted.	As for Medium Risk
Ensuring appropriate access to information	In line with the Corporate Acceptable Use Policy, personal log- ins and passwords must not be shared with anyone under any circumstances.	As for Low Risk, plus Computer screens must not be left on view to prevent unauthorised individuals from seeing information not intended for them. • Lock screens when not working at them using the Lock Session function (Windows key + L) • If sharing screens using Microsoft Teams, ensure all information on the screen can be shared and the recipients are entitled to access it. • Consider the visibility of on-screen information through ground floor windows. Rearrange angle of screen and/or desk if necessary.	As for Medium Risk
Destroying electronic data	County Council hard drives to be returned to IT for cleansing and disposal. Return encrypted USB sticks to Helpdesk for reallocation.	As for Low Risk, plus Remove information from encrypted USB sticks and return them to Helpdesk for reallocation.	As for Medium Risk

SECURE EMAILING AND OTHER METHODS OF ELECTRONIC TRANSMISSION			
	LOW RISK	**MEDIUM RISK (Including Personal Data)**	**HIGH RISK (Special Category Data and High Risk Business Information)**
Sending electronic information to colleagues within the County Council	Do not use any personal (non-HCC) email accounts for work-related emails.	As for Low Risk, plus Emailing between @hants.gov.uk email addresses is permitted. Mark email as “Confidential” as appropriate (in new email toolbar, Tags, More Options, Sensitivity dropdown). Further information can be found on the IT Security pages. Mark email as “Private” to prevent anyone else from seeing the email. Please note that any emails marked “Private” that are sent to a shared inbox can only be seen in the O365 online version of Outlook.	As for Medium Risk
Deciding how to send electronic information outside the Council	Regularly delete any old and unused email addresses from the Outlook picklist to prevent them being used accidentally. Do not use any personal (non-HCC) email accounts for work-related emails.	As for Low Risk, plus Large volumes of medium risk data should be sent encrypted. Emails can be encrypted by marking them as “confidential”. In new email toolbar, click Tags, select More Options (arrow in bottom right), and select “Confidential” in the Sensitivity dropdown. Further information can be found on the IT Security pages. From April 2020, @hants.gov.uk email addresses meet required government security standards. It is not necessary for staff to use separate @private.hants.gov.uk or @nhs.net accounts.	As for Medium Risk High risk information should be sent encrypted. Emails can be encrypted by marking them as “confidential”. In new email toolbar, click Tags, select More Options (arrow in bottom right), and select “Confidential” in the Sensitivity dropdown. Further information can be found on the IT Security pages.

Preparing information for electronic transmission	If you are sending a mailing out to people at their personal email addresses, these email addresses are personal information and should not be shared between the recipients. Use BCC to keep these hidden. Copy email addresses rather than manually typing these where possible. Do not use any personal (non-HCC) email accounts for work-related emails.	As for Low Risk, plus If there are file attachments, check you have included the correct attachments by opening each of them before sending. Apply Data Protection principles: send a minimum of personal information and on a need-to-know basis, anonymise where possible. Double check that you have selected the correct email address(es) before sending and remember to encrypt where appropriate (see above).	As for Medium Risk plus Ask someone else to check your email is completely correct before sending it if possible (chosen addresses, correct attachments).
File transfer applications (such as Dropbox, WeTransfer, and SafeDrop)	Any application used to transfer County Council data must have been through the DPIA process for that use of the data. There is no Corporate DPIA due to the variety of purposes involved and the local management required. This method should be used as an exception for large files that are too large to email. When sharing links, follow the principles of sending by email.	As for Low Risk, plus: Check you have included the correct link by opening it before sending. Apply Data Protection principles: send a minimum of personal information and on a need-to-know basis, anonymise where possible. Double check that you have selected the correct email address(es) before sending.	As for Medium Risk. Ask someone else to check your email is completely correct before sending it if possible (chosen addresses, correct links to files).

Electronic working away from the office	Keep your device up to date, ensuring you install all required security updates to prevent potential hacking. Lock your screen (Windows key + L) when it is not in use to prevent access to any systems.	As for Low Risk, plus If you have access to an HCC-issued device, you can use this to access Hantsnet Modern. If you are using your own device, use the online O365 applications and the business applications portal to access HCC data securely. If you wish to access the County Council email & calendar information from a mobile device you must use the Microsoft Mobile Apps and follow the security requirements. Consider the security of your working from home/away from the office setup. Try to prevent your screen from being visible to other members of your household or other people that may be nearby.	As for Medium Risk
Secure use of shared/open Outlook calendars	No specific requirements	Do not include personal information or sensitive business information in meeting requests or calendar details. Calendars can be viewed by all people who have a Hantsnet logon – not just County Council staff – and any external organisations that you may have shared your calendar with. Mark appointments as private if the subject is sensitive. Hold a minimum of personal information in the body of calendar appointments (use initials if necessary), no case details. Convey information in a parallel email if necessary. Use links to SharePoint documents, with the appropriate security settings applied.	As for Medium Risk

A2.3 Verbal information

	LOW RISK	MEDIUM RISK (Including Personal Data)	HIGH RISK (Special Category Data and High Risk Business Information)
Secure telephone use outside the office	No special requirements.	If in a public place, do not disclose information by phone where you can be overheard. Use headphones where possible to reduce the information that could be overhead. If you cannot find a sufficiently private location for your call, postpone the conversation.	As for Medium Risk
Secure telephone use in the office	No special requirements.	Consider who is around you when making telephone calls and exercise discretion in what is said, applying the principles within the UK GDPR (see above). Do not include information at this level of sensitivity in a voicemail message or convey it to anyone other than the intended recipient (including family members, carers or guardians) unless you have confirmation that they have the authority to act on behalf of the involved person.	As for Medium Risk plus If information is very sensitive, take the conversation to an alternative location e.g. a meeting room or quiet area.
Receiving incoming telephone calls	No special requirements.	Do not share personal and/or special category information with a caller unless checks have been done to confirm they are who they say they are. • Where the caller is a frequent contact, the caller may be recognised by their voice. • Otherwise, it is recommended that the caller be asked to confirm key facts about themselves that we hold (e.g. address or date of birth).	As for Medium Risk
Holding conversations outside of the office.	No special requirements	Consider who may be around you and could overhear. Hold the conversation in a more private location where appropriate.	As for Medium Risk

A2.4 Recordings – secure use of video, including calls, meetings and Live Events

	LOW RISK	MEDIUM RISK (Including Personal Data)	HIGH RISK (Special Category Data and High Risk Business Information)
Meetings with service users/clients	N/A – all call/meeting recordings will include personal data – video of attendees, names, and/or contact details	All attendees must be made aware that the call/meeting will be recorded prior to the call/meeting taking place. All attendees must be advised of the purpose of recording including lawful basis, how the information is held, who it may be shared with, and the appropriate retention period. This must be done via a Privacy Notice specific to this purpose. All recordings must be transferred to the appropriate data storage facility (e.g. SharePoint) and the appropriate retentions applied. Any recordings may be subject to requests under UK GDPR, which could include disclosure of the recording to the data subject.	As for Medium Risk If the meeting is very sensitive, carefully consider the appropriate storage location.
Internal meetings with staff	N/A – all call/meeting recordings will include personal data – video of attendees, names, and/or contact details	All attendees must be made aware that the meeting will be recorded prior to the meeting taking place. All attendees must be advised of the purpose of recording, how the information is held, who it may be shared with, and the appropriate retention period. This must be done via a Privacy Notice specific to this purpose. All recordings must be transferred to the appropriate data storage facility (e.g. SharePoint) and the appropriate retentions applied. If minutes are being taken separately, consider whether a recording is required. If minutes are being transcribed from the recording, the recording should be deleted once this has been completed if they are no longer required for another purpose. Any recordings may be subject to requests under UK GDPR, which could include disclosure of the recording to the data subject.	As for Medium Risk plus If the meeting is very sensitive, carefully consider the appropriate storage location.

Meetings including external organisations	N/A – all call/meeting recordings will include personal data – video of attendees, names, and/or contact details	All attendees must be made aware that the meeting will be recorded prior to the meeting taking place. All attendees must be advised of the purpose of recording, how the information is held, who it may be shared with, and the appropriate retention period. This must be done via a Privacy Notice specific to this purpose. All recordings must be transferred to the appropriate data storage facility (e.g. SharePoint) and the appropriate retentions applied. If minutes are being taken separately, consider whether a recording is required. If minutes are being transcribed from the recording, the recording should be deleted once this has been completed if they are no longer required for another purpose. Any recordings may be subject to requests under UK GDPR, which could include disclosure of the recording to the data subject.	As for Medium Risk If the meeting is very sensitive, carefully consider the appropriate storage location.
Live events	N/A – will include personal data – video of presenter, names, and/or contact details	Hide the identity of any audience members to prevent personal data being accidentally shared. All attendees must be made aware that the event is being broadcast live.	As for Medium Risk If the subject matter is very sensitive, this should not be broadcast

A2.5 Potential data protection incidents

	LOW RISK	MEDIUM RISK (Including Personal Data)	HIGH RISK (Special Category Data and High Risk Business Information)
What to do if information may have been lost or compromised	Not applicable.	**Step 1:** Immediately contact their line manager or key Council contact. **Step 2**: Take steps to retrieve the information, including: • Attempting to recall an email sent to the wrong person(s) internally • Ask the recipient to delete an email they have incorrectly received • Contacting the recipient of wrongly disclosed information and asking them to return the information, or collecting them yourself • Retracing your steps or searching the immediate area for mislaid paper documents. **Step 3:** Make sure the County Council's Information Governance Team is informed **as soon as possible** using the Reporting a Data Incident Form. This is sent to data.protection@hants.gov.uk and the Departmental Data Protection Co-ordinator will be informed. A **Reporting a Data Incident Form must be completed, please provide as much information that you have at that time, but do not delay in submitting it even if you do not have all of the information.** **Step 4:** Contact the IT Service Desk on 01962 847000 if this relates to an IT system or device. **Step 5:** The County Council will then implement the procedures for investigating and assessing the incident outlined further in this document.	As for Medium Risk