group policies and procedures

# Data protection policy

|  |  |
| --- | --- |
| Category | Information Governance |
| Author | Castleman Healthcare Ltd |
| Responsible Director | Fiona Pickering |
| Date of issue | September 2021 |
| Next review date | September 2023 |
| Document ref & version | Data Protection Policy September 2021 |

**Related policies and guidance**

**Document revision and approval history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approved by | Comments |
| V1 | July 16 |  |  |  |
| V2 | Sept 16 |  |  | Changes made |
| Final | Sept 16 |  |  | Includes information sharing policy information |
|  | April 18 |  |  | Reviewed by JL. |
|  | Dec 18 |  |  | Links to GDPR added |
|  | Aug 19 |  |  | Reviewed by JL |
|  | Sept 2021 |  |  | Reviewed and amended by FP |

# aim

Castleman Healthcare Ltd conforms to the Data Protection Act and GDPR legislation by ensuring that appropriate consent is obtained, information is processed and limited to patient care, records are stored in secure locations and all staff are aware of their role in relation to the requirements of the Act. The purpose of this policy is to build on the guidance contained within the Information Governance overarching policy incorporating GDPR and provide specific guidance relating to compliance with the new GDPR legislation and to Information Sharing in particular.

It links to Castleman Healthcare Ltd’s overarching Information Governance Policy which sets out the minimum policy standards for confidentiality, integrity and availability of information. It covers the overlapping areas of data protection compliance (including Caldicott), information security (ISO27002 – Code of Practice for Information Security), data quality, confidentiality (with regard to ‘common law’), records management and compliance with legislative requirements such as Data Protection Act 1998, Freedom of Information Act 2000, GDPR and other related legislation that is relevant to information handling.

Castleman Healthcare Ltd has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty to comply with guidance issued by the Department of Health, NHS England, other advisory groups to the NHS and guidance issued by professional bodies.

# INTRODUCTION TO THE LEGISLATION

In response to the requirements placed on EU Members States by the European Data Protection Directive, the UK Government enacted the Data Protection Act 1998 which received Royal Assent in July 1998. The main provisions of the Act came into force on 1 March 2000 with certain transitional provisions coming into effect on 24 October 2001. The impact on Healthcare organisations was summarised in the Caldicott Report of 1997. This identified key principles governing the use of Patient Identifiable Data. Much of this was either superseded or entwined with the General Data Protection Regulation which came into force in May 2018.

The fundamental purpose of GDPR is to protect people's privacy by preventing unauthorised or inappropriate use of their personal details. While it is a highly complex piece of legislation, putting it into practice boils down to complying with the eight Data Protection Principles (which are detailed in paragraph 3 below) and ensuring that we: -

1. Are validly registered as a Data Controller and have a Data Protection Officer in post.
2. Hold no more information about individuals than is necessary for patient care or employment purposes and obtain necessary consents to using patient data for any marketing purposes.
3. Store records (both paper and electronic) securely and confine access to authorised personnel.
4. Comply with individual's legitimate requests for access.
5. That the Company has in place data sharing agreements and data processing impact assessments.
6. Ensuring that all patient data transmitted from practices to Castleman Healthcare Ltd. is anonymised.

Although many similarities exist between this Act and the previous 1984 Data Protection Act, which is now repealed, there are some important differences.

# GDPR – general data protection regulation

## **At a glance**

* The GDPR contains explicit provisions about documenting the Company’s processing activities.
* Castleman Healthcare must maintain records on several things such as processing purposes, data sharing and retention.
* Castleman may be required to make the records available to the Information Commissioners Office (ICO) on request.
* Documentation can help Castleman Healthcare comply with other aspects of the GDPR and improve your data governance.
* Controllers and processors both have documentation obligations.
* For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
* Information audits or data-mapping exercises can feed into the documentation of processing activities.
* Records must be kept in writing.
* Most organisations will benefit from maintaining their records electronically.
* Records must be kept up to date and reflect Castleman Healthcare’s current processing activities.

## **CASTLEMAN CHECKLIST FOR COMPLIANCE**

**Documentation of processing activities – requirements**

* we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the GDPR.
* we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the GDPR.

We process special category or criminal conviction and offence data, we document:

* the condition for processing we rely on in the Data Protection Act 2018 (DPA 2018);
* the lawful basis for our processing; and
* whether we retain and erase the personal data in accordance with our policy document.

where required in schedule 1 of the DPA 2018.

* We document our processing activities in writing.
* We document our processing activities in a granular way with meaningful links between the different pieces of information.
* We conduct regular reviews of the personal data we process and update our documentation accordingly.

**Documentation of processing activities – best practice**

When preparing to document our processing activities we:

* do information audits to find out what personal data our organisation holds;
* distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and
* review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

* information required for privacy notices;
* records of consent;
* controller-processor contracts;
* the location of personal data;
* Data Protection Impact Assessment reports; and
* records of personal data breaches.

We document our processing activities in electronic form so we can add, remove and amend information easily.

### **What’s new under the GDPR?**

* The documentation of processing activities is a new requirement under the GDPR.
* There are some similarities between documentation under the GDPR and the information provided to the ICO as part of registration under the Data Protection Act 1998.
* We make sure that we have in place a record of our processing activities.

### **What is documentation?**

* Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; this is called **documentation**.
* Documenting our processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help us demonstrate our compliance with other aspects of the GDPR.

### **Who needs to document their processing activities?**

* Controllers and processors each have their own documentation obligations.
* There is a limited exemption for small and medium-sized organisations. As Castleman Healthcare has less than 250 employees, we need only document processing activities that:
  + are not occasional; or
  + could result in a risk to the rights and freedoms of individuals; or
  + involve the processing of special categories of data or criminal conviction and offence data.

### **What do we need to document under Article 30 of the GDPR?**

* The name and contact details of our organisation (and where applicable, of other controllers, our representative and our data protection officer).
* The purposes of our processing.
* A description of the categories of individuals and categories of personal data.
* The categories of recipients of personal data.
* Details of our transfers to third countries including documenting the transfer mechanism safeguards in place.
* Retention schedules.
* A description of our technical and organisational security measures.

### **Should we document anything else?**

As part of our record of processing activities, it can be useful to document (or link to documentation of) other aspects of our compliance with the GDPR and the UK’s Data Protection Act 2018. Such documentation may include:

Information required for privacy notices, such as:

* + The lawful basis for the processing.
  + The legitimate interests for the processing.
  + Individuals’ rights.
  + The existence of automated decision-making, including profiling.
  + The source of the personal data.
* Records of consent.
* Controller-processor contracts.
* The location of personal data.
* Data Protection Impact Assessment reports.
* Records of personal data breaches.

Information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018, covering:

* + The condition for processing in the Data Protection Act.
  + The lawful basis for the processing in the GDPR; and
  + Our retention and erasure policy document.

### **How do we document our processing activities?**

* Doing an information audit or data-mapping exercise can help us find out what personal data our organisation holds and where it is.
* We can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of our organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.
* When documenting our findings, the records we keep must be in writing. The information must be documented in a granular and meaningful way.

# Roles & responsibilities

**Castleman Healthcare Ltd Board**

It is the role of Castleman Healthcare Ltd Board to define the Information Governance framework, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the framework, taking advice as and when required from the Information Governance Lead and any sub-committees.

**Corporate Governance Director**

The Director with delegated responsibility for Information Governance in Castleman Healthcare Ltd has overall accountability and responsibility for Information Governance and is required to provide assurance that all risks to Castleman Healthcare Ltd, including those relating to information, are effectively managed and mitigated. Castleman Healthcare Ltd has also appointed a Data Protection Officer.

The Data Protection Officer for Castleman Healthcare (sometimes also known as the privacy officer) is the designated contact with the Information Commissioner on behalf of Castleman Healthcare for all data protection issues. The main features of this role will be to provide advice and support to Castleman Healthcare whilst leading on audit and improvement plans relating to information governance. The Data Protection Officer is responsible for maintaining Castleman Healthcare’s data protection notification with the information Commissioner and ensuring the Company’s on-going compliance with the Data Protection Act 1998, including advising the Caldicott Guardian on points of interpretation, particularly where issues arise as a result of the interface between the Act and the use of technology. If the DPO is also the Caldicott Guardian, the Governance Director will provide any advice and support to them.

**Caldicott Guardian**

The Caldicott Guardian is the executive with Board level responsibility to ensure Castleman Healthcare Ltd complies with the Data Protection Act 1998 and the GDRP legislation. This role gives both support to the Information Governance Director with a direct channel to progress issues, and emphasises to all staff the importance of implementing and ensuring compliance with statute.

The Caldicott Guardian is responsible for compliance with the Caldicott principles. The role is responsible for establishing and maintaining procedures governing access to, and the use of, patient identifiable data held or processed within systems or networks which are the responsibility of Castleman Healthcare ltd. The Guardian will also agree local procedures and protocols to ensure consistency with any relevant central requirements and guidance.

# THE DATA PROTECTION PRINCIPLES

The nine Data Protection Principles are:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processes in any manner incompatible with that purpose or 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 processes for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures should be taken against unauthorised or unlawful personal processing of personal data, against accidental loss or destruction of or damage to personal data.
8. Personal data should 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.
9. Any patient data should be annonymised if transmitted between practice and Castleman Healthcare ltd.

# THE RIGHTS OF DATA SUBJECTS

Under the Data Protection Act 1998, individuals ("data subjects") have numerous statutory rights. GDPR legislation also reinforces this.

These include a right to:

1. Prevent processing likely to cause damage or distress.
2. Request that accurate data be rectified, blocked, erased or destroyed.
3. Prevent processing for direct marketing purposes.
4. Claim compensation or damage for distress caused by any breach of the Act.

The Act also provided additional safeguards for the processing of 'sensitive data' (e.g. patient health records). This has significant implications for the processing of patient data throughout Castleman Healthcare Ltd, particularly the issue of patient consent to process their data and use it for non-clinical purposes (e.g. the used of addresses to send mail shots to market the unit's services).

# DATA PROTECTION AUDIT

In keeping with our core values, it is important that we ensure that there is full compliance with the provisions of the Data Protection Act 1998 and GDPR legislation throughout Castleman Healthcare Ltd.

With this in mind, Caldicott Guardian and Governance lead will regularly review the impact and implications of the Data Protection Act on Castleman Healthcare Ltd as part of the audit process.

In summary, the objectives of the audit are to:

1. Compare the business processes of Castleman Healthcare Ltd against those required as a result of the introduction of the Act and associated legislation.
2. Prepare a comprehensive data protection risk assessment for Castleman Healthcare Ltd from which to identify the key factors to ensure improvement.
3. Decide priority actions to address the primary issues emerging from the analysis
4. Update this policy as required.

# GENERAL GUIDANCE

The Data Protection Act and GDPR requires that any patient information received by a Castleman Healthcare Ltd member of staff must be:

1. Processed fairly and lawfully.
2. Held only for a specific purpose (i.e. for imaging and ancillary documentation).
3. Not disclosed in any other manner.
4. Adequate and relevant.
5. Kept up to date.

Staff are to be aware that a breach of this Act could empower the Registrar of Data Protection to enter Company premises and search, upset, examine, operate and seize any data equipment and files.

The data which carries the greatest risk of possible breaches of the Act are:

1. Patient's clinical and financial/administrative records.
2. Personal data on consultants and other medical practitioners in respect of their practice privileges or contractual arrangements with Castleman Healthcare Ltd.
3. Human Resources data and personal information concerning employees.

# ACCESS TO HEALTH RECORDS

The adoption of formal policy and resulting good practice for the sharing of information with key stakeholders will lead to confidence in Castleman Healthcare Ltd, its commissioning bodies and the general public. Effective information exchange is the key to the safe delivery of clinical care. Sharing information meets the requirements of statutory and local initiatives and is vital for coordinating services between partner organisations. Appropriate information sharing builds trust and good relationships between partners.

Responsible information sharing brings together services that reveal a more accurate picture of an individual’s health. The streamlining of information sharing enables care to be delivered quickly, efficiently, safely and accurately. It also enables commissioners and providers to get a greater level of understanding about how services are operating across the borough. Overall, this improves analysis, decision-making, resource allocation and better use of public funds.

Barriers to effective information sharing include:

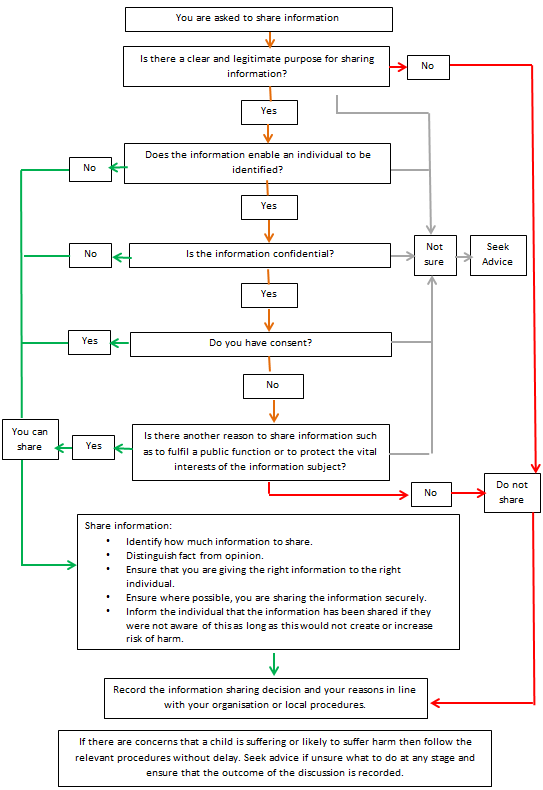
1. Misconceived ideas, particularly data protection legislation.
2. A lack of guidance and plain language explanations.
3. An absence of formal protocols between partners.
4. A tendency to take an overly cautious approach.
5. A lack of awareness of the benefits.

Castleman Healthcare Ltd will ask for and keep information, so that patients receive correct care and treatment when needed and for as long as they need it.

Castleman Healthcare Ltd also needs to share information to ensure:

1. That all services meet patients’ needs, now and in the future.
2. That payment terms are fulfilled correctly.
3. That cross – organisation pathways can be reviewed and high standards maintained.
4. Recognition of staff training requirements and educational needs.

Each time Castleman Healthcare Ltd is asked or wishes to share information, the following thought process is undertaken (as taken from the *Information Sharing: Practitioners’ guide*, HM Government, 2015)



Due to the nature of business, there is only a few occasions where Castleman Healthcare Ltd has a need to share or request information from other bodies. The movement of person identifiable information is documented on the internal patient information flow chart, including Safe Haven locations. For details on how to safely share information with NHS or other organisations, please refer to the Information Governance Policy.

Other than for legal purposes, Castleman Healthcare Ltd does not share person identifiable data.

**See Subject Access Record Policy & Fair Processing Notice for further guidance.**

# Safe Haven

Castleman Healthcare Ltd will ensure that access to confidential information is strictly controlled to minimise the risk of unauthorised access to this information, whether accidental or deliberate.

Castleman Healthcare Ltd will implement Safe Haven procedures to safeguard confidential information flowing to, within and from the organisation so that all such information exchanged passes between Safe Haven contact points.

All Castleman Healthcare Ltd employees transmitting confidential information must identify and use their relevant Safe Haven contact points and inform their recipients of these Safe Haven procedures to ensure compliance.

Castleman Healthcare Ltd will ensure that all members of staff are aware of the existence of the Safe Haven principles and the policies and procedures surrounding it.

Staff should familiarise themselves with the Caldicott Principles to protect themselves and their clients, as follows:

* 1. Principle 1 Justify the purpose(s)for using confidential information.
  2. Principle 2 Only use it when absolutely necessary.
  3. Principle 3 Use the minimum necessary patient-identifiable information.
  4. Principle 4 Access should be on a strict need-to-know basis.
  5. Principle 5 Everyone must understand their responsibilities.
  6. Principle 6 Understand and comply with the law.

**7.2 Letters**

Please send patient identifiable information through the relevant internal/external postal system using the confidential letter envelopes applicable to the appropriate commissioner organisation wherever practicable.

If not practicable, please mark the envelope SAFE HAVEN – CONFIDENTIAL: RETURN TO SENDER IF UNDELIVERED. Ensure the sender’s address is legible.

**7.3 Telephone**

Confirm the identity of the other party prior to discussing confidential issues or divulging confidential details

**7.4 E mail**

Patient identifiable data must only be sent by e-mail in a method approved by the Caldicott Guardian. The following method is approved:

The only secure way of sending personal identifiable information electronically is from one nhs.net email to another nhs.net account, or nhs.uk to another nhs.uk. This complies with the ‘best practice’ recommendations from Connecting for Health. This NHS mail email service is unique because the e-mail is encrypted in transit. For more details, view <https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email>

**7.5 Electronic – via e-mail using Microsoft protected attachment**

Patient identifiable data must only be sent by e-mail in a method approved by the Caldicott Guardian. This method is approved but only as ‘good practice’ as Microsoft e-mail is not a secure transmission process.

1. Create a source file (Word usually but could be Excel) to contain the required confidential information.
2. Save the document as ‘Save as’; highlight on the word ‘tools’ (find it on the top tool bar) left click and it will show a drop-down list: select ‘Options’ then ‘Security options’; select ‘Password to open’ and type in this box a password that you must remember; select o.k.; on next screen select ‘Save’.
3. Create a new e-mail in the normal way and type a clear subject header.
4. Use the ‘insert’ tab on the top toolbar and paste your password protected confidential file into this e-mail as an attachment.
5. Write whatever non-confidential text you wish but make sure you advise your recipient to a) contact you for the password and b) remove the attachment from their e-mail once they have opened it.
6. Ensure that you finish this e-mail with your signature showing a clear contact number that enables the recipient to get hold of you on the day.
7. When your recipient contacts you, confirm their identity and tell them the password so that they can read the file containing the confidential information.

# MANAGERS AND DEPARTMENT LEAD RESPONSIBILITIES

Managers are asked to check that:

1. Existing policies on the control and release of patient and employee occupational health records are observed.
2. Patient data (i.e. their names and addresses) is not used for marketing purposes (e.g. mail shots) unless there is confidence that the individuals concerned have consented to the use of their personal information for marketing purposes. (The admission form currently in use has a box in which patients may indicate that they do not wish to receive details of Castleman Healthcare Ltd services; the adequacy of the current wording will be examined as part of the data protection audit.)
3. Staff, especially front-of-house staff, are briefed on how to respond to a request from an individual (under the provisions of the Act) for details of the personal data that Castleman Healthcare Ltd holds on them. It is recommended that in the first instance such requests be referred to a member of the Senior Management Team, pending the issue of advice on the handling of such requests.

# HUMAN RESOURCE INFORMATION AND DATA PROTECTION

**1 Rights of the Individual under the Date Protection Act(s)**

1. To be able to access one's own personal data.
2. To be able to claim compensatory damages, or losses caused by the use of inaccurate data or unauthorised use of data or by the loss or destruction of data.
3. To apply to the courts if necessary for rectification or erasure of inaccurate data.

The Company adopts the following strategy for the safe keeping of human resources material:

**2 Human Resource files**

1. The HR records for Castleman Healthcare Ltd are kept under lock and key with the Director of Personnel.
2. Two people can access this information including:
   1. The Director of Personnel lead.
   2. Relevant named manager.
3. The file remains locked unless two designated managers are in the office at the time the files are being examined.
4. Only information relevant to an individual's employment are kept.
5. Data is only held for specified and lawful purposes.
6. No inappropriate disclosure is permitted.
7. Personal data must be accurate.
8. Personal data must not be kept longer than necessary.

**3 Computer and Paper Files kept by the Company**

1. Staff absence.
2. Staff sickness.
3. Retire on ill-health.
4. Dismissals.
5. Staff turnover record.
6. Working hours’ record.
7. Paternity/Maternity.

# CONFIDENTIALITY

Corporate Policy is to strictly maintain the principles of confidentiality of patient information. The instances in which patient information can be revealed are:

* In private discussions with colleagues.
* Where waived by the patient.
* In discussions in a "group practice".
* Where obtained by statutory agencies (such as Child Protection etc) for data processing (i.e. statistic gatherings).
* Where disclosure is required by law, i.e. for Misuse of Drugs Act, etc.
* Where the information is stored for record-keeping only.
* Where a doctor needs to defend him/herself, e.g. against accusations made by the GMC.

# FURTHER INFORMATION

A Fact Sheet for staff is attached as **Appendix 2.**

Further information is available from:

Information Commissioner's Office

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire

SK9 5AF

Telephone: 0303 123 1113 Fax: 01625 524510

E-mail: [icocasework@ico.org.uk](mailto:icocasework@ico.org.uk)

Website: <https://ico.org.uk/>

# appendix 1 - WHO IS A 'HEALTH PROFESSIONAL'?

In the Data Protection Act 1998 "health professional" means any of the following:

1. A registered medical practitioner (a "registered medical practitioner" includes any person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section).
2. A registered dentist as defined by section 53(1) of the Dentists Act 1984.
3. A registered Optician as defined by section 36(1) of the Opticians Act 1989.
4. A registered Pharmaceutical Chemist as defined by Section 24(1) of the Pharmacy Act 1954 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976.
5. A registered Nurse, Midwife or Health Visitor.
6. A registered Osteopath as defined by section 41 of the Osteopaths Act 1993.
7. A registered Chiropractor as defined by section 43 of the Chiropractors Act 1994.
8. Any personal who is registered as a member of a profession, to which the Professions Supplementary to Medicine Act 1960 for the time being extend.
9. Clinical Psychologist, Child Psychotherapist or Speech Therapist.
10. Music Therapist employed by a health service body, and
11. Scientist employed by such a body as head of department.

# appendix 2- FACT SHEET - DATA PROTECTION ACT 1998 - GUIDANCE FOR STAFF

The Data Protection Act has been in full effect from 24th October 2001. The biggest change since the 1984 Act is that the act covers paper/manual records as well as computer records.

**The 1998 Act works in two ways:**

**1.** It gives individuals the right to know WHY information about them is being collected.

**2.** It also says that those who record and use personal data must be open about HOW information is used and to follow the 8 principles overleaf.

The Act is for all and, therefore, affects you personnel record as well as patient notes.

**Castleman Healthcare Ltd believes that we should ensure that everyone's individual data stays confidential.**

Data is anything that can be traced back to an individual.

**How does this affect you?**

* All patients should have a copy of the Patients Guide which includes details of the Data Protection Act, on their first visit/contact/admission.
  + All records and personal data must be held securely.
  + Clear desks at night including diaries.
  + Do not take patient information home.
  + Lock windows and doors.
  + All laptops must be encrypted.
* No databases should be created containing patient identifiable information without notification to the Data Controller.
* Staff need to be kept up to date on any patient requests for their data not to be passed on.
* All staff must have a contract signed with a security and confidentiality clause in it.
* Keep your passwords confidential, ensure they contain both letters and numbers. Log off your computer when you have finished or lock it by pressing CTRL, ALT and DEL when you leave your desk.
* Email - do not use identifiable information as the message or document name.

**The 8 Principles of Good Information Handling**

**1.** Data should be fairly and lawfully processed.

**2.** Data should be processed for limited purposes.

**3.** Data should be adequate and relevant and not excessive.

**4.** Data should be accurate and, where necessary, kept up to date.

**5.** Data should be processed in accordance with individual's rights.

**6.** Data should not be kept longer than is necessary.

**7.** Data should be secure.

**8.** Data should not be transferred to countries without adequate protection.

**Definitions**

Processing under the new Act means the obtaining, recording or holding of information or data or carrying out any operation or set of operations on the information or data.

Personal data covers both facts and opinions about the individual.

Sensitive data includes racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions. Sensitive data can only be processed under strict conditions, which include:

* Having the explicit consent of the individual.
* Being required by law to process the data for employment purposes.
* Needing to process the information in order to protect the vital interests of the data subject or another.
* Dealing with the administration of justice or legal proceedings.

**Individual's Rights in relation to the 5th Principle**

1. Right of an individual to access data.
2. Right to prevent processing likely to cause damage or distress.
3. Right to prevent processing for the purposes of direct marketing.
4. Rights in relation to automated decision making.
5. Right to take action for compensation if the individual suffers damage or distress.
6. Right to take action to rectify, block, erase or destroy inaccurate data.
7. Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.