Information Governance

First name:

Surname:

Company:

Date:

Please complete the above, in the blocks provided, as clearly as possible.
Completing the details in full will ensure that your certificate bears the correct spelling and date.
The date should be the day you finish & must be written in the DD/MM/YYYY format.

Copyright Notice

Information Governance

Contents

N.B: We are aware that official practice is to use the terms “service users” or “people using this service” to describe those receiving care. We prefer the term “client” and use it throughout our training package.

Key:

worksheet

important

example

Information Governance

Learning outcomes.

- **Understand the need for agreed ways of working.**
- **Identify relevant legislation.**
- **Understand confidentiality and when to share information.**
- **Recognise data protection principles.**
- **Identify the need for clear recording.**
- **Know how to report concerns about the recording storage and sharing of information.**

Fundamental standards.

The fundamental standards are the standards by which CQC will inspect social care. The standards are based on the regulations from the Care Act 2014 and CQC have changed the focus for the purposes of inspection.

The fundamental standards are those standards that no care setting must fall below.

The standards are based on five areas as follows:

Safe.	People are protected from abuse and avoidable harm.
Effective.	People's care, treatment and support show quality of life and promote good outcomes, and providers should show evidence to prove it.
Caring.	Care should be person centred involving dignity and respect, and compassion.
Responsive.	Following correct working procedures as agreed by your workplace and as set out in the client's care plan.
Well led.	Management leadership and governance should ensure all of the above happens. Staff training should be recognised and openness and fairness be apparent.

These areas are known as key lines of enquiry or KLOES. Each KLOE has a set of criteria which CQC use to check whether the fundamental standards are being met.

Information Governance

The fundamental standards are as follows:

Person centred care.	Ensuring that those receiving the care are at the centre of all decisions.
Dignity and respect.	Providing the client with dignity and respect in all aspects of their care.
Need for consent.	Asking the client's permission before carrying out tasks that affect them.
Safe care and treatment.	Following correct working procedures as agreed by your workplace and the client's care plan.
Safeguarding service users from abuse.	Following agreed working and safeguarding procedures and being aware of signs and symptoms.
Meeting nutritional needs.	Being aware of dietary needs, working with the care plan, ensuring clients have the right equipment and conditions to eat.
Cleanliness, safety and suitability of premises and equipment.	Carrying out required checks of premises and equipment, implementing cleaning rotas and carrying out safety checks.
Receiving and acting on complaints.	Having a complaints policy and procedure in place that is accessible to all and act in accordance with the policy when dealing with complaints.
Good governance.	Ensuring that all aspects of the workplace is overseen and policies and procedures are implemented and monitored regularly.
Staffing.	Fit and proper persons employed. Fit and proper person requirement for Directors is followed.
Duty of candour.	Relevant information must be volunteered to all persons who have or may have been harmed by the provision of services, whether or not the information has been requested and whether or not a complaint or a report about that provision has been made.

Our Redcrier manuals will provide your staff with training to support attainment of the fundamental standards.

Information Governance

Introduction.

Handling information is a big part of your role, it is also a big responsibility as much of the information will be confidential. We now have more ways to communicate than ever before including social media and mobile devices such as mobile phones and laptops. Although this makes it easier to share things with many people quickly, it also means that there is more chance of information being sent to the wrong people by mistake.

Breaches of confidentiality are very serious in any workplace, so it is important that you know what your workplace policies are regarding storage, use, disposal and sharing of information.

This manual will help you to understand relevant legislation, such as the Data Protection Act 2018, which includes the General Data Protection Regulation (GDPR), and the Protection of Freedom Act. It will also look at confidentiality and sharing information as well as the need to ensure records are clear and up to date.

If you are completing the care certificate, the information in this manual will help you with your knowledge and understanding.

Information Governance

Unit One

What is information governance?

Information governance is a term used to describe the systems and processes in the storing, handling and use and sharing of personal information held on an individual. Data controllers (those responsible for the holding of personal data and information) have a statutory duty to ensure that it is held secure, is relevant and used for the purpose for which it is being held. Information Governance applies to both data and information.

Data is about factual statements and numbers, so for instance it may be the number of clients who your workplace supports.

Information is the interpretation or representation of data, for instance the detail about those clients such as who they are, information about them and how they use your service. There are generally two types of information.

Personal information This can be things such as name, address etc.

Confidential personal information, this is more detailed Information such as might be in a care plan or medical record.

Information governance links data protection with the Caldicott principles, information security and information confidentiality. In the care sector, information governance ensures safeguards and appropriate use of personal information.

Every client that uses your workplace should feel secure in knowing that their personal and confidential information is protected. They should also feel that those providing their care are using their information appropriately and only when necessary.

Make a list of the types of information your workplace needs to keep in order to provide a quality care service.

Data controller: public authority or other body. They decide how and why data is processed.

Data processor: a body that processes data for the controller. In many care organisations they may be both deciding what data they need and processing it.

There are a number of pieces of legislation that have relevance to your workplace and impact on information Governance. They are as follows:

The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

This Act sets out the fundamental standards that all health and social care providers must meet to satisfy Care Quality Commission registration criteria.

To meet appropriate standards in your workplace you should have the following in place:

- Adequate training for all staff.
- Policies and procedures / agreed ways of working.
- Appropriate recording systems.
- Relevant risk assessments.
- Good communication with other services providing care to your clients.

Regulation 17 of this Act states:

- The registered person should be able to assess, monitor and improve the quality and safety of the services they provide.
- Assess monitor and avoid or reduce any risks to the health and safety of those using the service.
- Maintain an accurate and up to date record of each person using the service and keep it securely.
- Maintain records of those carrying out the regulated activities.

The Care Act 2014.

The Care Act aims to build on good practice in the Health and Social Care Act as well as embedding new reforms to provide clearer and fairer care and support to those who need it. The Care Act provides for a more person centered approach in social care as well as putting a greater focus on prevention and wellbeing.

The principle of wellbeing underpins the Act and should be considered in all decision making for individuals. A duty of candour has been placed on all providers ensuring they are open and honest in all of their dealings with their clients including how they will use any personal or confidential information.

Information Governance

The Care Act aims to put people firmly in control of their own care and support and producing plans for their care. This will help to improve independence and wellbeing and ensure all aspects of a person's life are supported. Local authorities will also need to ensure there are a wide variety of care provisions and services and that information, advice and advocacy are available as needed. Ensuring that information collected throughout all of these processes is accurate, used and stored and shared appropriately is key to the health and wellbeing of all involved.

Protection of Freedoms Act 2012.

As well as providing guidance for creating a multi agency approach to safeguarding which should be referred to when creating policies and procedures for safeguarding, this Act also gives people the right to ask for information from public authorities and puts a duty on public authorities to publish certain information about their activities. Public authorities include government departments, NHS, Health and Safety executive etc. If you work in an organisation that must comply with the Act you should know who is responsible for handling requests, and what the procedure is as there is a 20 day turnaround.

Local Guidance Documents.

All local authorities have been given the brief to co-ordinate agencies to work together to safeguard adults and children. This will involve the necessity to share information at times

Data Protection Act 2018.

This Act controls how our personal information is used by organisations, businesses or the government. Everyone who uses data must follow a set of principles to ensure safe handling, use and storage. This prevents information from falling into the wrong hands which could increase the likelihood of abuse. The Data Protection Act has 8 principles to guide us when using other peoples information.

The principles are:

1. Personal data shall be processed fairly and lawfully and shall not be processed unless at least one of the following conditions have been met:

- The person has given consent.
- There is a contract in place with the person.
- It is part of the process required to enter into a contract.
- It is necessary for the vital interests of the person e.g. Administration of justice.

Sensitive personal data shall be processed fairly and lawfully and shall not be processed unless at least one of the following conditions have been met:

- Person has given explicit consent.

- It is necessary to protect the persons vital interests even though they are unable to give consent.

2. Used for limited specifically stated purpose.
3. Used in a way that is adequate, relevant and not excessive.
4. Accurate.
5. Kept for no longer than is absolutely necessary.
6. Handled according to peoples data protection rights.
7. Kept safe and secure.
8. Not transferred outside of the European economic area without adequate protection.

The Data Protection Act is regulated by the Information Commissioners Office. They can offer advice, guidance, promote good practice, monitor breach reports, conduct audits, monitor compliance and take enforcement actions.

General Data Protection Regulations (GDPR).

The Data protection Act has been updated, with its main purpose being to implement the General Data Protection Regulations, GDPR, to give citizens and residents back control of their personal data. GDPR will affect all businesses in some way.

It applies to large businesses but will also apply to small businesses under 250 employees, if the processing carried out is likely to result in a risk to the rights and freedom of data subjects, the processing is not occasional, or the processing includes special categories of data as defined in GDPR Article 9.

Article 9.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation shall be prohibited unless you have consent from the person in question or it is for employment purposes.

How personal data is kept, used, stored and shared will need to be transparent. This means that when personal data is collected, the individual needs to know the purpose it is being used for, how you will keep it safe and who you will share it with if it is applicable.

The right to be forgotten.

As well as having a duty to let people know what we are going to do with the information we have about them, we also need to be aware that under GDPR, customers can withdraw their

consent to us keeping information, this is known as the right to be forgotten. This cannot be honoured whilst they are in a legal contract or there is a legal obligation that their information is retained, such as to comply with official authority, needed in defence of a legal claim or if it is in the public interest, such as for health purposes, research or archiving purposes.

Subject Access Requests.

Under Data protection, individuals have the right to ask to see any personal information that is held on them. The organisation holding the information must enable this to happen, unless they have justification not to. If the information held is not up to date, they may be in breach of data protection. The information must be in a recognised format.

Breaches of GDPR can result in fines and / or claims being pursued by the individual. Leaving the EU will not affect the introduction of GDPR as the government have said they will use the basis of these regulations to prepare our own regulations after Brexit.

A client has given consent to your workplace holding information on them, what do they need to know in return?