Official

Information Governance Framework

Applies to	All employees of Achieving for Children and all individuals or organisations acting on behalf of Achieving for Children.
Date created	January 2016
Most recent review	September 2020
Signed off by	Information Governance Board
Reviewing arrangements	The policy will be reviewed every two years to judge its effectiveness or updated sooner in accordance with changes in legislation.
Next review date	August 2022
Equality analysis completed	Not required
Relating policies and procedure (including tri-x chapter)	Information Governance Policies and Procedures
Version	3.0
Version History	January 2016 - approved by Director of Standards and Improvement May 2018 - updated to comply with GDPR. Approved by Director of Standards and Improvement September 2020 - updated to incorporate new IG policies and service changes. Approved by Information Governance Board

1. Introduction

Information is a vital asset for the provision of services to the public and for the efficient management of services and resources. It is therefore of paramount importance to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability provide a robust information governance framework.

Information Governance consists of a framework of overarching roles and responsibilities, policies, standards, procedures and guidance that covers all information disciplines and all information created, received, managed, shared and disposed by Achieving for Children. Failure to ensure Achieving for Children policies and procedures reflect the requirements under the Data Protection Act 2018 and the General Data Protection Regulations 2016 can expose the organisation to significant risk of enforcement notices, monetary penalties, media exposure and or loss of services alongside criminal proceedings.

Information governance applies to all personal, confidential and corporate information, regardless of format, function or location.

2. Purpose

This policy defines a robust information governance framework that enables Achieving for Children to meet the key requirements of legislation, including the General Data Protection Regulations (GDPR), government standards and established best practice.

3. Information Governance Objectives

The objectives of the information governance framework are to:

- maintain policies, procedures and guidance for each information discipline where required;
- maintain an up to date and complete information asset register for information assets held by Achieving for Children;
- identify, assess and mitigate risks to information assets;
- integrate information governance principles into all relevant organisational processes;
- ensure compliance with relevant legislation, codes of practice and government standards;
- ensure the quality of data os that it can be used to drive service design and delivery; and
- inform staff of Achieving for Children about information governance requirements and their responsibilities

4. Information Governance Principles

We are committed to the development of high quality information governance across Achieving for Children and to establishing a culture which properly values, protects, supports and uses data and information. There are give interlinked principles which guide the application of this information governance framework:

- Quality assurance
- Legal compliance
- Information security
- Proactive use of information
- Openness and transparency

4.1 To ensure information quality assurance, Achieving for Children will:

- establish, maintain and promote policies and procedures for information quality assurance and effect management of records;
- undertake or commission assessments and audits of its information quality and records management arrangements;
- ensure that key service user data is accurately recorded and maintained, including regular cross checking against source data;
- ensure that managers as Information Assets Owners (IAOs) are required to take ownership of, and seek to improve the quality of information within their services and that information quality is assured at the point of collection; and
- ensure that appropriate reports and records are maintained in line with the requirements to capture and assess processing activities.

4.2 To ensure legal compliance, Achieving for Children will:

- regard all identifiable personal information relating to customers and employees as confidential except where national requirements on accountability and openness require otherwise;
- establish and maintain policies or procedures to ensure compliance with relevant law and regulation including the GDPR, Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality and all associated guidance; and
- establish and maintain policies or procedure for the controlled and appropriate sharing of information with other agencies, taking into account relevant legislation (e.g. Children's Act, Crime and Disorder Act) or any other requirement for data sharing in accordance with national contracts and or public tasks

4.3 To ensure that appropriate and legal compliant information security exists, Achieving for Children will:

- establish and maintain an Information Security Policy along with respective procedures for effective policing and secure management of all its information assets, resources and IT systems;

- undertake and or commission assessment and audits of its information and IT security arrangements inline with said policy;
- promote effective confidentiality and security practices to ensure all permanent and temporary, contracted employees and third party associates of Achieving for Children adhere to this via appropriate laid down policy procedures, training and information awareness activities/documentation
- establish and maintain appropriate incident reporting procedures and monitoring and investigations of all instances, actual and or potential, along with any reported breaches of confidentiality, security or data protection principles;
- identify and classify information to ensure that it is handled and shared appropriately; and
- ensure effective reports, processes and records are in place to provide information asset owners with the ability to identify risks and take actions.

4.4 To ensure proactive use of information, Achieving for Children will:

- ensure Achieving for Children embeds and monitors data protection by design by proactively assessing changes to the way we create, use, store and or share information;
- ensure systems are in place to recognise information assets and owners;
- ensure systems and processes are in place to recognise, identify and take action against information risks;
- ensure information systems hold the information required to support service user focused service delivery and operational management;
- develop information systems and reporting processes which support effective performance management and monitoring;
- develop information management awareness and training programmes to support managers in using information to manage and develop services; and
- ensure that, where appropriate and subject to confidentiality constraints, information is shared with other organisations in order to support improved service delivery

4.5 To ensure openness Achieving for Children will:

- ensure that non confidential information about Achieving for Children and its services is readily and easily available through a variety of media in line with Achieving for Children's Publication Scheme;
- implement policies to ensure compliance with the Freedom of Information Act and the Environmental Information Regulations;

- ensure that service users have readily and easily available access to information relation to Achieving for Children services, and their rights as service users;
- have clear procedures and arrangements for liaison with the press and broadcasting media and customer; and
- ensure appropriate privacy notices are in place to capture the requirements of the GDPR in providing data subjects with adequate and appropriate information over the way in which Achieving for Children collects, processes and shares information while ensuring the rights of individuals are clearly identified.

5. Legal and Regulatory Framework

There are a number of legal obligations placed upon Achieving for Children for the use and security of personal identifiable information including:

- General Data Protection Regulation (EU) 2016/679
- Freedom of Information Act 2000
- Local Government Act 1972
- Public Records Act 1958 (where not superseded by the Freedom of Information Act)
- Data Protection Act 2018 (and subsequent Special Information Notices) (Currently being removed)
- Human Rights Act 1998
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Re-use of Public Sector Information 2003 (EU Directive)
- Public Interest Disclosure Act 1998
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health and Safety at Work Act 1974
- Transparency Code
- Health and Social care legislation such as:
    - NHS Sexually transmitted disease regulations 2000
    - National Health Service Act 1977
    - Human Fertilisation and Embryology Act 1990
    - Abortion Regulations 1991
    - Health & Social Care Safety and Quality Act 2015 (Applicable to Adult Social care only)

To manage its obligations, Achieving for Children will issue and support policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.

6. Information Governance Policies

The Achieving for Children Information Governance Framework is addressed in three parts, information security, information rights and records management (Figure 1).

The policies and procedures under these three areas are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, sharing and destruction of all data and records held or used by Achieving for Children and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery. It will also censure that measures are in place to reduce the occurrence of breaches in information security.

Figure 1

7. Governance arrangements

The information governance structure is led by the Information Governance Board. The Board consists of senior officers from services across the organisation and promotes a culture of good record management and data security and ensures compliance with data protection legislation and other legislation related to information governance.

The Board is chaired by the Senior Information Risk Officer (SIRO) and also attended by the Information Governance Lead (Data Protection Officer) and the Head of Business Systems and ICT to ensure compliance of the regulations is upheld.

The Information Governance Board is responsible for ensuring that any risks identified are addressed and for providing assurance to the Chief Operating Officer and Director of Finance, Achieving for Children Board and the commissioning councils that the organisation takes information management and governance seriously and can demonstrate visible improvements through a risk based approach. The terms of reference and members are available via this link

7.1 Roles and responsibilities for implementing, monitoring and reviewing

Roles	Responsibilities
Senior Information Risk Owner	Is accountable for information risks, fosters a culture for protecting and using data appropriately and provides senior responsibility for managing information risks and incidents and is concerned with the management of all information assets.
Caldicott Guardian	Is advisory and acts at the conscience of the organisation. Provides a focal point for service user confidentiality and information sharing issues. Is concerned with the management and sharing of personal information. The two Directors of Children's Services in Achieving for Children are the Caldicott Guardians for their respective operational areas.
Information Governance Lead	The Information Governance Lead shall have overall responsibility for managing and implementing the Framework and related policies and procedures on a day to day basis. The Information Governance Lead ensures that Achieving for Children has adopted good information governance policies and procedures and complies with data protection laws. The function will also act in an advisory capacity to the Caldicott Guardian and SIRO where required. The Information Governance Lead which also acts as the Data Protection Officer for Achieving for

	Children in its statutory function.
Head of Business Systems and ICT	Responsible for developing, implementing and reviewing policies and procedures to protect Achieving for Children's network and information assets, providing advice and guidance on information and cyber security. The role will also input into general user awareness and training and is responsible for data security initiatives generally.
Information Governance Support Officers	Responsible for complying with data subject requests and freedom of information requests, developing, implementing and enforcing records management practice across Achieving for Children. The role is also responsible for delivering reports to the IG Board that cover the requirement for data processing, information assets and audit outcomes alongside regulatory compliance.
Information Asset Owners (IAO)	Designated senior officers with ownership and responsibility for specific information assets (paper based and electronic records and IT systems). The IAO must identify and document the availability requirements for their systems and formulate a contingency plan in the event of system failure supported by the Information Asset Custodians.
Information Asset Custodian	Designated Officer with responsibility for day to day management and protection of specified information assets (paper based records and IT systems)
Line Managers	Are responsible for ensuring that their permanent and temporary employees and contractors have: ● read and understood this Framework and the policies and procedures applicable in their work areas ● been made aware of their personal responsibilities and duties in relation to information governance ● been made aware of who to contact for further advice ● received appropriate and up to date training related to information governance ● abide by Achieving for Children code of conduct

8. Strategic Implementation

The Information Governance Board will monitor implementation of this framework through regular meetings which involve:

- ensuring the development and review of policies and procedures required for information governance and having final approval of these document;
- ensuring appropriate resources are in place to achieve compliance of the regulatory requirements; and
- reporting on progress, incidents and issues to the Chief Operating Officer/ Achieving for Children Board

This Framework will be reviewed bi-annually or as required in responsible to any significant legislative changes, mandatory requirements, national guidance or as a result of significant information governance breaches or incidents and approved by the Information Governance Board.

Information Asset Owners will be a key part of this process as they are the officers accountable for information assets across the council and are responsible for ensuring that appropriate information governance arrangements are in place local and that national or legal requirements are met.

7. Governance and Compliance

Non-compliance with the Information Governance Framework could potentially expose Achieving for Children and or service users to risk. The potential impact of damage or loss of information includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence, or media coverage and may take considerable time and costs to recover.

Non compliance with these policies and procedures may lead to disciplinary action in line with Achieving for Children's disciplinary procedures and or legal action if appropriate.

A short fact sheet is included in Appendix 3 to help Achieving for Children employees comply with Information Governance policies.

8. Training

Prior to new employees being given full access to Achieving for Children's ICT systems they are required to complete a series of short training modules to introduce Achieving for Children's approach to Information Governance. The modules are available to employees through CPD Online. These modules are available to all Achieving for Children staff and must

be completed within the first week of staff starting with Achieving for Children. The modules required for completion include:

- Data Protection Awareness Training
- Stay Safe Online Training(Cyber Security)

Appendix 1

Information Governance Checklist

Keeping children, young people, families, employees and other personal information secure

- keep passwords secure – change regularly and do not share with anyone.
- lock (ctrl,alt,del) or log off computers when away from desks.
- ensure computer screens are sited away from the view of others to prevent unlawful disclosure of sensitive information.
- secure confidential paper waste securely in the confidential bins provided.
- prevent virus attacks by taking care when opening email and attachments or visiting websites.
- work to a 'clear desk' basis – by securely storing hard copy personal information when it is not being used.
- maintain an awareness of who should be allowed in areas normally restricted to employees and to keep those areas secure.
- if personal or sensitive data is held on any portable storage device – e.g. laptop, USB pen, it must be encrypted.

Meeting the reasonable expectation of the people whose data we handle

- collect only the personal information you need for a particular business purpose.
- records should be updated promptly to ensure accuracy.
- only view information for a legitimate business purpose.
- you may be committing an offence if you are disclosing information without consent – this includes verbal disclosure – offences may lead to disciplinary action.
- inform the Caldicott Guardian or Information Governance Lead of any potential Information Sharing Agreements.
- when transporting personal data ensure that it is kept secure at all times.
- records in all formats should be stored, handled and retained in accordance with the Records Management Policy.

Disclosing personal information

- check that information held is accurate and up to date - especially name and address information.
- incorrectly addressed mail is our most common form of accidental disclosure.
- be aware that there are people who will try to trick you to give out personal information.
- to prevent disclosures you must be 100% confident you know who you are speaking to, especially to someone making an incoming call.
- ensure that sensitive conversations are not overheard by others.
- when leaving answer phone messages, you should not disclose sensitive information – just leave your name and contact details.