Information Governance Policy

Scope of this Policy:	**All Staff**
Approved by:	**Niall Kelly**
Date Ratified:	**28 July 2020**
Next Review Date (by):	**August 2021**
Version Number:	**2020/02**

VERSION CONTROL	
VERSION	**DATE**
Version 1	12th June 2019
Version 2	28th July 2020

POLICY SUMMARY/PURPOSE/RATIONAL

This document explains:

- Why this policy is necessary (**rationale**)
- To whom it applies and where and when it should be applied (**scope**)
- The underlying beliefs upon which the policy is based (**principles**)
- The standards to be achieved (**policy**)
- How the policy will be met through working practices (**process**)
- Links to other agencies

Table of Contents

1. PURPOSE AND RATIONALE

Purpose –

To explain the roles, responsibilities and process for the management of risk across all & Young Foundations (YF) services, homes and schools.

This policy details how the organisation complies with the legal requirements of the General Data Protection Regulations which supersede the DPA and become legally enforceable from 25th May 2018. It sets out the procedural principles for managing confidential and sensitive data processed by the organisation ie any information that is produced, held and stored by the company (data processing).

Rationale –

To ensure that the organisation critically examines and effectively manages all risks to people, structures, finances and all other assets, including reputation, in such a way as to avoid where possible, or reduce, harm, damage or other losses, which could affect the ability of the organisation to carry out its normal activities

In order to be considered as a well-led organisation with robust governance systems the organisation needs to be able to demonstrate that it has clearly described information risk management processes in place.

The policy is also a fundamental component of YF's quality assurance and clinical governance processes.

Information Governance and the individual's right to confidentiality are important issues for YF. The handling and processing of confidential data is a daily activity for the company and it is committed to ensuring that data is handled securely and that the risk of any data breach is minimised.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 Aims

The aim of this policy is to ensure that:

- All staff are aware of their responsibilities under the General Data Protection Regulations
- Staff adhere to good practice outlined by the Eight Principles of Data Protection
- Anyone handling personally identifiable information (PII), sensitive personal data and/or company sensitive data is appropriately trained and supervised
- There are clear procedures for handling personal information
- All staff are aware of the consequences of data breaches and mishandling of information

2.2 Objectives

- To demonstrate YF's commitment to handling Personally Identifiable Information and commercially sensitive data in a fair, responsible manner which fully complies with current legislation
- To provide staff with clear guidance on meeting their legal responsibilities regarding processing data
- To minimise risks to individuals and to the organisation, including financial and reputational risks

3. SCOPE

As an <u>all staff</u> document, this policy applies to all staff employed by *Young Foundations* (whether on a permanent or temporary contract).

The Information Governance Policy should be implemented and monitored by all Registered / Service Managers, supporting functions and services.

4. DEFINITIONS

4.1 The following definitions are provided to support understanding in relation to this policy:

Data	Any information which is processed by automatic or manual means, recorded so that it can be processed by automatic or manual means or recorded for the purpose of filing and/or storage.
Personally Identifiable Information (PII)	Any Information relating to an identified or identifiable natural person
Sensitive Personal Data	Any personal data consisting of information as to: (a) the racial or ethnic origin of the data subject; (b) their political opinions; (c) their religious beliefs or other beliefs of a similar nature; (d) whether they are a member of a trade union; (e) Genetic/Biometric data (for the purpose of uniquely identifying a natural person) (f) their sexual life or sexual orientation; (g) a person's health
Data Subject	The individual named within the data or who is the subject of personal data
Data Controller	The person or organisation (usually the organisation) that determines the purpose and means of the processing of personal data.
Data Processor	A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller
Processing	Processing of data means "obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data"
Data Management System	Any manual or computerised system that stores or processes data, for example: Payroll system, Incident reporting system.
Database	Any medium, manual or digital, that stores data in an organised and accessible format, for example; Spreadsheets, SQL Databases etc.

5. PROCESS

RESPONSIBILITIES

Management Responsibilities

5.1. Overall responsibility for the secure handing of data rests with the Data Controller. The Data Controller, in the case of YF, is the company. The Board is accountable for and responsible for ensuring that the organisation has an effective Information Governance and Data Protection policy and strategy, taking into account relevant legal requirements and guidelines. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy and overall strategy.

5.2. The Data Protection Lead for YF is Liz Prowse, Data Protection Officer. This role includes:

- Providing guidance for data protection issues
- Maintaining registration
- Ensuring management and staff are aware of their responsibilities under the policy

It is the day to day responsibility of all staff and in particular the Registered Managers and Department Leads to ensure that effective data protection procedures are adhered to. Systems and protocols are required to ensure the safe processing of data that are both practicable and appropriate to each service. Regular monitoring and appraisal of the systems are required to ensure continued improvement in Data Management processes.

Information Governance Training

5.3. Managers will ensure that they and all their staff have received information governance training and that this is refreshed annually. This may be online (where available) or via face to face training.

External Contractors

5.4. All third party contractors with access to confidential information owned by or held by YF are required to sign a temporary contract and/or provide evidence of their own Data Protection Policy or procedures. The contract must include an appropriate clause outlining contractors' responsibility for the confidentiality of information they have access to or otherwise comes to their attention. Contractors should be made aware of the procedures for reporting actual or suspected confidentiality breaches.

New or changed systems or services

5.5. All new processes, services, information systems, and other key information assets must comply with information quality and confidentiality and data protection requirements. Managers and senior staff will liaise with information governance staff to ensure that confidentiality issues have been identified and appropriate control measures are or will be in place. This must be carried out at an early stage in the project cycle. Consideration must be given as to whether a Privacy Impact Assessment is needed.

Quality of personal information

5.6. For personal information to be of use it is essential that it is accurate and up to date. YF will ensure the quality of information by:

- Validating and confirming information with students and residents
- Informing students and residents about the importance of providing accurate information
- Ensuring that all staff who obtain and record student or resident information record it accurately, legibly and fully
- Giving students and residents the opportunity to check information held about them
- Encouraging students and residents to inform staff if any of their details have changed
- Introducing monitoring procedures to check the accuracy and quality of data

Staff Responsibilities

5.7. Staff must have read, understood and signed the YF Information Governance Policy. In particular:

- Staff must adhere to the principles set out in this policy
- Staff must report immediately any concerns relating to the processing of any data or breaches of data. All cases of near miss or actual breaches of confidentiality must be recorded as incidents using YF's incident reporting procedure
- Staff must be aware of their responsibilities to process and handle data securely and to use company procedures to ensure that they fulfil their responsibility in full
- Staff must ensure that they log out of any electronic devices when they are not in use and ensure that they are secured safely when not required
- Staff must ensure that documents are kept secure, eg in offices with restricted access, or in locked cabinets when not in use and that

workspaces are kept free from confidential information when unattended

Legislation

5.8. Data Protection applies to all personal information whether in manual files, electronic files, computer databases, documents, video or other 'automated' media such as personnel and payroll records. Effective from May 25th 2018 the Data Protection Act is superseded by the General Data Protection Regulations (GDPR). This new legislation focuses on the Rights of individuals – known as Data Subjects.

5.9. Under GDPR there are 7 guiding Principles and 8 Data Subject 'Rights'. The company has to, by law, register its use of data with the Office of the Information Commissioner (ICO), outlining the purposes for holding data, how it is used and to whom it may be disclosed.

GDPR Principles

- **Principle 1 - Legality, Transparency & Fairness**

  Any kind of Personal Data must be processed in accordance with the rules and guidelines of the GDPR, and whilst doing so must state the grounds upon which it is processing Personal Data; Any kind of information an Organisation passes to the individual about the way it processes their data must be disclosed early and thoroughly, it must be in an accessible and obtainable manner, it must be freely provided; In order to execute the rights of the Data Subject, the Data Controller must implement the protection procedures for the Data Subject. The principle of 'fairness' includes Data Subjects 'Rights' of which there are 8.

- **Principle 2 - Purpose Limitation Principal**

  Personal data should be collected for specified, legitimate and explicit purposes, and must not be further processed in a way which is incompatible with such purposes.

- **Principle 3 - Minimisation Principle**

  Personal data must be relevant, adequate and limited to what is necessary in relation to the purpose for which those data are processed.

- **Principle 4 - Accuracy Principle**

  Personal data must always be accurate and up to date. Actions should be taken to avoid storing old redundant data. Actions must be taken to ensure that inaccurate personal data, with regard to the purpose for which they are processed, should be erased or rectified without delay.

- **Principle 5 - Storage Limitation Principle**

  Personal data shall be: Kept in a form that permits identification of the Data Subject for no longer than is necessary for the purposes for which the personal data is processed; Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- **Principle 6 - Integrity and Confidentiality Principle**

  Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

- **Principle 7 - The Accountability Principle**

  The Data Controller shall be responsible for, and be able to demonstrate compliance with, Principles 1-6 above.

5.10. Other relevant policies/procedures are:

- Online Social networking guidelines
- Electronic Communication and Internet guidelines
- Mobile Communication Equipment guidelines
- Clear desk guidelines
- Subject Access Request
- Records Management Policy

5.11. The company regards all identifiable personal information relating to individuals as confidential and individuals have an expectation that personal information provided by them will be held in confidence. This duty of confidence exists even if the individual is unable to give information actively eg, because of severe learning disability, lack of capacity or unconsciousness.

Implementation Process

5.12. The data protection lead has overall responsibility for maintaining awareness of confidentiality and security issues for all staff. Training is co-ordinated by the training department and will cover the following subjects:

- Personal responsibility
- Confidentiality of personal information
- YF policies and procedures relating to data protection
- Compliance with General Data Protection principles

- Good practice guidelines
- Awareness of the role of the data protection lead and how they can be contacted

Induction of new staff will follow a similar format. In addition nominated staff will be given additional training to support them in their roles where necessary.

5.13. Staff contracts will include a GDPR and confidentiality clause. Agency and interim staff are governed by the same rules. All staff are required to sign a copy of their contract stating that they are aware of their responsibility under the GDPR. Any breach of Data Protection regulations could result in the member of staff facing disciplinary action.

Disclosure of Sensitive personal information

5.14. There are certain circumstances defined by acts of parliament (outlined below) that govern the disclosure and/or sharing of sensitive personal information. Some make it a legal requirement to disclose and others state that information cannot be disclosed.

5.15. Sensitive personal information includes information regarding:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Genetic/Biometric data
- Sex life/Sexual Orientation
- A person's health

5.16. Legislation to restrict disclosure of personal information:

- Human Fertilisation and Embryology (Disclosure Of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations Of 1974 and 1992
- Abortion Act 1967
- Children and Adoption Act 2006

5.17. Legislation requiring the disclosure of personal information:

- Public Health (Control of Diseases) Act 1984 and the Public Health (Infectious Diseases) Regulations 1985
- Education Act 1996 (sec 520 - for immunisations and vaccinations to NHS trusts from schools)

- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Electronic Data

5.18. Much of the data produced and controlled by YF is processed electronically. Electronic Data is any information that is stored digitally and includes text, video, photographs, images or scanned documents. Examples of this are:

- E-mail - all internal and external e-mails
- Service User information such as letters, treatment plans
- Payroll records including staff names, addresses and salaries
- HR information such as qualifications, telephone numbers
- Financial information such as company accounts

5.19. Key principles to follow in managing electronic data:

- Only equipment issued by YF can be used for processing company data. This equipment includes, but is not exclusive to computers, laptops, mobile telephones, Blackberries.
- All data stored by the company must be held on the company server on either the network drive or personal drive, or on other company approved storage systems such as a backup systems.
- All e-mail correspondence must be made by an approved YF e-mail address.
- All equipment issued by YF will be secured by a PIN or Password known only to the user.
- All equipment must be kept secure at all times. It is the responsibility of the individual staff member to whom the equipment was issued to ensure its safe keeping. In particular, where staff have been issued with electronic devices and these are transported in a vehicle, they are not to be left in the vehicle unless locked in the boot or glove box of that vehicle.
- No confidential personal or company information shall be stored on any device, including but not limited to, computers, data sticks, external hard drives, 'cloud' based systems.
- Information is only to be processed on equipment issued by YF, including but not limited to, personal computers, data sticks, zip drives, external hard drives, 'Cloud' storage systems, mobile telephones and smart telephones.
- No personal or sensitive personal data should be sent to an unsecure source. Senders should contact the recipient before sending any

information and agree an appropriate secure method. This includes e-mails and attachments. Once an appropriate secure method has been agreed this should be followed for that and all future communications.

- No confidential correspondence shall be made using personal or other unauthorised e-mail address.
- No member of staff shall disclose their PIN or password to another member of staff.
- 'Logged in' Terminals should not be left unattended.
- No software can be installed onto company issued devices unless authorised by the company.
- Where possible avoid printing or creating other 'hard' copies of electronic data as they will be subject to non-electronic data control (see below)

Non-electronic Data

5.20. Young Foundations produces a variety of paper documents and notes which contains both personal data, sensitive personal data and company sensitive data. Non Electronic data is anything that is stored on a physical medium such as paper records, photographs and white boards. Examples of this are:

- Young person's notes such as clinical assessments, or other therapeutic materials
- Written correspondence both clinical and non-clinical
- Meeting notes and minutes
- Correspondence received by the company
- Application forms
- Estates records

5.21. Key principles to follow in managing non-electronic data:

- When not in use, all non-electronic data must be kept secure using a company approved filing system
- Manual records must not be left unattended in any unsecure public areas
- Offices where manual records are stored must remain secure against unauthorised access
- Manual records must not be shared with any unauthorised third party
- If manual records require transmission by fax the sender must contact the recipient before sending to ensure that the information is

sent to a 'Safe Haven' fax and to confirm the information has been received securely

- A local procedure must be in place for when records are required to be taken away from their usual point of storage. For example, service users attending hospital appointments
- When staff are required to escort service users and take a copy of service user records, the member of staff must ensure security of the records at all times
- Staff must not discuss personal data, sensitive personal data or company sensitive information with anyone who does not have a legitimate reason for knowing that information or in public areas
- Non-electronic records must not be left unattended in any unsecured public areas
- Non-electronic records should not be left unattended in a vehicle unless they have been securely locked in the glove or boot of the vehicle

Photography

5.22. Photography means the recording of any pictorial images by any means including, but not limited to, photographic film, digital imaging and video.

In order to protect the confidentiality, privacy and dignity of students and residents, photography on YF premises or while on YF business must be strictly controlled. Prior permission must be sought and obtained from the home or school manager for the taking of photographs.

Photographs of individuals must not be taken without their written, informed consent. It is essential that only individuals who have given written consent are included in any photograph. If the individual does not have capacity to give their consent then photographs must not be taken.

Data Breach

5.23. **Electronic data -** A breach of electronic data includes: loss or theft of a computer or mobile telephone or other company approved storage device, the transmitting of data to an unsecure recipient, the transmitting of data to the wrong recipient, unauthorised access to a YF device.

5.24. **Non-electronic data -** A breach of non-electronic data includes: theft or loss of notes or any other non-electronic records and inappropriate disclosure of personal data or sensitive personal data.

5.25. What to do in the event of an actual or suspected data breach

- The member of staff who has identified or is responsible for the data breach must immediately take action to minimise the risk of any further data breaches occurring;
- The member of staff must immediately inform their line manager who shall then inform the Data Protection Officer and the company's Senior Information Risk Owner (SIRO)
- The incident shall be reported as normal using the company's incident reporting procedures;
- Where the data breach involves personal data or sensitive personal data, consideration will be given by the Data Protection Lead as to whether the Information Commissioner's Office needs to be informed.

6. TRAINING AND SUPPORT

6.1 **Implementation Plan** - all policy documents will need an implementation plan which:

(a) identifies

(i) the tasks to be completed,

(ii) the date these tasks will be completed by,

(iii) the person(s) responsible for completing the task(s);

(b) and takes account of:

(i) which staff need to be briefed;

(ii) whether additional training and / or ongoing training is required as part of a member of staff's Personal Development.

7. IMPACT ASSESSMENT EQUALITY AND HUMAN RIGHTS ANALYSIS

7.1. Equality and Human Rights

YF recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The organisation is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The organisation believes that all people have the right to be treated with dignity and respect and is committed to the

elimination of unfair and unlawful discriminatory practices.

YF also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

7.2 Impact assessment

IMPACT ASSESSMENT

Policy Title: The Policy on Policies
Area covered: *all areas, all staff*

Who will be affected? *staff*

Evidence
Disability (including learning disability)
Sex
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*
Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*
Language *The need for additional language presentation e.g. Welsh, English etc.*
Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.*
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.*
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.*

Equality & Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	*Use not engaged if Not applicable*
Right of freedom from inhuman and degrading treatment (Article 3)	*Use supportive of a HRBA if applicable*
Right to liberty (Article 5)	
Right to a fair trial (Article 6)	
Right to private and family life **(Article 8)**	
Right of freedom of religion or belief **(Article 9)**	
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	
Right freedom from discrimination **(Article 14)**	

8. FURTHER READING/GUIDANCE

9. APPENDIX 1

There are 8 rights of the Data Subject under GDPR alongside 7 Principles articulated in section 5.9

Right 1 – Right to Be Informed

The right to be informed covers your necessity to provide fair processing information. This is typically through a Privacy Notice. It places emphasis on the need for transparency over how Personal Data is used.

The information you supply depends on how the personal data was acquired and whether it was directly through the individuals or not.

The material you give regarding the processing of Personal Data must be:

- *Concise, Transparent, Understandable and easily accessibple*
- *Communicated in clear and plain language*
- *Free of Charge*

Right 2 - Right of Access (Subject Access Request)

Under GDPR, individuals will have the right to obtain:

- *Confirmation that their data is being processed*
- *Access to their personal data*
- *Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice*
- *The mechanism for this is called a Subject Access Request (SAR)*

Right 3 - Right to Rectification

- *Data Subjects are entitled to have their Personal Data corrected if it is inaccurate or incomplete*
- *If you have disclosed the PII to 3rd parties*
    - *You must inform them of the correction (where possible)*
    - *You must also inform the Data Subject which third parties have the information*
- *You must respond within one month*
    - *The period of compliance may be extended by a further 2 months. This is in cases where the requests are complex or multiple*
    - *In such an instance, the individual must be informed within one month of the receipt of the request and an explanation as to why the extension is necessary*
- *If action is not taken in response to a request for rectification, adequate reasoning explaining why must be communicated along with informing the requestor about their right to contact a Statutory Authority or a judicial remedy.*

Right 4 - Right to Erasure

- *The right to erasure does not provide an absolute 'right to be forgotten'*
- *Individuals have a right to have their personal data erased and to prevent processing in some specific situations, these include:*
    - *When the personal data is no longer necessary regarding the purpose for which it was originally collected/processed*
    - *When the individual withdraws consent*
    - *When the individual oposes the processing and there is no superseding legitimate interest for continuing the processing*
    - *If the personal data was unlawfully processed*
    - *If the personal data must be removed to comply with a legal obligation*
    - *If the personal data is processed in relation to the offer of information/society services to a child*

Right 5 – Right to Restrict Processing

- *When processing is restricted, it is possible to store the personal data, but you are not permitted to further process it*
    - *You can retain just enough information about the individual to guarantee that the restriction is respected in the future*
- *You will be able to restrict processing of personal data in the following circumstances:*
    - *Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data*
    - *Where an individual objects to the processing and you are considering whether your organisation's legitimate grounds outweigh those of the individual*
    - *If you no longer require the personal data but the individual requires the data to establish, exercise or defend legal claim*
    - *When processing is unlawful, and the individual opposes erasure and requests restriction instead*
    - *You may need to review procedures to make sure that you are able to determine where you may be required to restrict the processing of personal data*
    - *If you have disclosed the personal data in question to third parties, you must notify them about the restriction on the processing of the personal data. Exceptions are made if this is not possible or if it involves disproportionate effort to do so.*
    - *You must inform individuals when you decide to lift a restriction on processing*

Right 6 Right of Data Portability

- *The right of data Portability enables individuals to acquire and reuse their personal data for their own purposes across different services*
    - *This allows individuals to move, duplicate, or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.*

- *It allows consumers to take advantage of applications and services that can use this data to help them save money, or help them understand their spending habits*

- *The right of data portability only applies:*

Right 7 Right to Object

- *Individuals have the right to Object to:*
    - *Processing that is based on genuine interests or the performance of a tgask in the public interest/exerciseof official authority, including profiling*
    - *Direct Marketing*
- *Individuals must object on the 'grounds relating to his/her particular situation'.*
- *As well as general processing, specific rules exist for processing PII for Marketing or Scinetific Research*
- *If your processing activities fall into any of the above categories and are carried out online, it is essential that you offer an option for individuals to be able to object online.*

Right 8 - Rights Related to Automated Decision Making and Profiling

- *Safeguards for individuals are introduced by the GDPR to protect against the possibility that a harmful decision is made without human intervention*
    - *Such rights work similarly to those existing under the DPA*
- *Individuals possess the right not to be subject to an agreement when it:*
    - *Is focused on automated processing*
    - *Results in a legal or important impact on the individual*
- *Suitable safeguards must exist when processing personal data for profiling reasins you must:*
    - *Specify reasoning behind the process and provide a breakdown of the possible consequences to guarantee fair and transparent processing*
    - *Adopt suitable statistical/mathematical procedures for profiling*
    - *Implement suitable administrative and technical actions for the purpose of minimising risks and to prevent discrimination.*
- *Individuals must be able to:*
    - *Acquire human intervention*
    - *Articulate their opinion*
    - *Receive an explanation of the arrangement and be able to challenge it*
- *Automated decisions adopted for the purposes listed in Article 9 (2) must not involve/implicate a child, or be based on special categories of data processing unless:*
    - *The explicit consent of the individual (or guardian) is evident*
    - *The processing is needed for the purposes of public concern on the basis of EU/Member state law – this must correspond with the aim of the task, respect the importance of the right to data protection, and determine appropriate functions to safeguard individual rights and interests*

10. APPENDIX 2

Information Governance Management Framework

The IG Management Framework provides a summary/overview of how YF is addressing the IG agenda. It is adapted to the planned capacity and capability of the organisation.

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement met by**	**Notes**
Senior Roles	• Senior Information Risk Owner (SIRO) • Information Governance Lead	The SIRO is Niall Kelly The Information Governance Lead is the Regulation and Compliance Officer.
Key Policies	• Information Governance and Management Framework Policy • Information Asset Risk Management Policy • Records Management Policy • Access to Records Policy • Online social networking guidelines • Electronic Communication and Internet Guidelines • Mobile Communication Equipment Guidelines • Clear Desk Guidelines • Network Security Policy	Policies set out scope and intent. Policies are ratified and reviewed by the Policy Review Group.
Key Governance Bodies	YF Directorate team and Service Managers	Information Governance is a function of YF's Quality Governance structure. Information Governance is a standing agenda item on YF's Board Meetings.
Resources	SIRO: Head of Regulation and Compliance IG Lead: Data Protection Officer Additional resources are provided as required.	Resources appropriate to Information Governance roles are allocated and reviewed at Board level.
Governance Framework	Responsibility and accountability for IG is cascaded throughout the organisation through staff contracts, third party contracts, IG training for all staff, quality governance	Clinical and care governance arrangements and IAOs monitor daily compliance with IG requirements.

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement met by**	**Notes**
	arrangements, Information Asset Owners.	
Training & Guidance	• Training for all staff • Training for specialist IG roles • Suite of IG guidelines	Staff have clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. Staff receive IG training applicable to their job roles. Training refreshed annually.
Incident Management	Incident Reporting policy is in place. All staff are aware of how to report incidents. All incidents are monitored by the DPO. Weekly and monthly incident reports are provided to the Board	Bespoke incident management software is in use for reporting and analysing all incidents.