

Data Protection Policy	
Author (s)	Narissa Leyland Head of Information Governance & Data Protection Officer
Corporate Lead	Leeds Community Healthcare NHS Trust Executive Director of Finance and Resources
Document Version	1.0
Document Status	Final
Date approved by Clinical and Corporate Policies Group (CCPG)	19 th March 2019
Date ratified by SMT	27 th March 2019
Date issued	2 nd April 2019
Review date	April 2022
Policy Number	PL378

Executive summary

Leeds Community Healthcare is committed to ensuring the privacy of individuals are respected and that all personal data processed is handled appropriately and in accordance with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA2018) and all other data protection laws collectively known in this policy document as (Data Protection Legislation).

The Trust has a legal obligation to comply with all appropriate legislation and guidance when processing personal data about patients, employees and other individuals.

DRAFT

Equality Analysis

Leeds Community Healthcare NHS Trust's vision is to provide the best possible care to every community. In support of the vision, with due regard to the Equality Act 2010 General Duty aims, Equality Analysis has been undertaken on this policy and any outcomes have been considered in the development of this policy.

Data Protection Policy

Contents

1. Introduction	4
2. Aims and Objectives.....	Error! Bookmark not defined.
3. Definitions	5
4. Responsibilities	6
5. GDPR Principles	8
6. Accountability	10
7. Lawful basis for processing.....	10
8. Consent	12
9. Individuals Rights.....	12
10. Data Processors and Contracts.....	13
11. Documentation	13
12. Data Protection by Design and Default	14
13. Data Privacy Impact Assessment (DPIA)	14
13. Data Protection Officer.....	14
14. Personal Data Breaches.....	15
15. International Transfers	15
16. Monitoring Compliance and Effectiveness.....	16
17. Training needs.....	17
18. Approval and Ratification process.....	17
19. Dissemination and Implementation.....	17
20. Review arrangements	17
21. Associated documents.....	17
22. References.....	17

1. Introduction

This policy is to set out the Trusts' commitment in how the organisation will comply with current Data Protection Legislation.

The Trust will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair and lawful collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information to the extent that it is needed to fulfil operational needs or to comply with legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

2. Scope

This policy must be followed by all staff who work for or on behalf of the Trust including those on temporary or honorary contracts, secondments, volunteers, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services.

The policy is applicable to all areas of the organisation and covers all aspects of information including (but not limited to):

- Patient/Client/Service User information.
- Personnel/Staff information.
- Organisational and business sensitive information.
- Structured and unstructured record systems - paper and electronic.
- Photographic images, digital, text or video recordings including CCTV.
- All information systems purchased, developed and managed by/or on behalf of, the organisation.
- Information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information.
- Retrieval, consultation, storage/retention or use of information.

- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons.
- Alignment, combination/linkage, blocking, erasing or destruction of information.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

3. Definitions

Data Protection Legislation refers to both the General Data Protection Regulations (2018) and the Data Protection Act 2018 where the following definitions apply.

Personal Data means ‘any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier’.

Special Category Data consists of personal data relating to:

- ethnic origin,
- physical and mental health (including, for example, details of the reasons for an individual’s sick leave),
- sexual preference,
- genetics
- biometrics (where used for ID purposes)
- religion or belief,
- political opinion
- Trade Union membership

Greater protections are required when processing this data.

Processing means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

Data Subject “Data subject” means an individual who is the subject of the personal data.

Data Controller means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means the Trust or nominated individuals acting on behalf of and with the authority of the Trust.

Data Processor means any person (other than a member of staff) or organisation that processes data on behalf of the Trust.

4. Responsibilities

Chief Executive

The individual with overall accountability for Information Governance within the Trust is the Accountable Officer, the Chief Executive. The role provides assurance, through a Statement of Internal Controls, that all risks to the organisation, including those relating to information, are effectively managed and mitigated, on a day-to-day basis will be delegated to the Head of Information Governance & Data Protection Officer.

Senior Information Risk Owner (SIRO)

The Trust has appointed the Executive Director of Finance and Resources as the Senior Information Risk Owner (SIRO).

The SIRO is responsible for:

- Taking overall ownership of the Trust's information risk management approach.
- Acting as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Trust's statement of internal control in regard to information risk.
- Implementing and lead the NHS information governance risk assessment and management processes.
- Advising the Board on the effectiveness of information risk management across the Trust.

Data Protection Officer

The Trust has appointed the Head of Information Governance and Data Protection Officer (DPO).

This role is defined under the EU General Data Protection Regulation (GDPR) 2018. The regulation specifies the minimum duties or "tasks" to be performed by the DPO.

- To inform and advise the Trust, and their employees, of their obligations under the Regulation and other applicable laws and regulations.
- To monitor compliance with the Regulation and other applicable laws and regulations and with the relevant policies of the Trust data controller, this includes assignment of responsibilities, awareness and training, and relevant audits.
- To advise on the data protection impact assessment (DPIA) and monitor its performance, if requested.
- To liaise with the Information Commissioner's Office as required under the GDPR (Article 39(1) (a-e)).
- The DPO will be the contact point for the public as regards the Regulation.

Information Security Manager

The Trust has appointed Head of Information Technology and the Head of EPR.

The Information Security Manager is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes of which the Data Protection Policy is one.

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Ensure that staff are aware of their responsibilities and accountability for information security.
- Be accountable to the SIRO and other bodies for Information Security across the Trust.
- Monitor potential and actual security breaches with appropriate expert security resource.

In carrying out these tasks the Information Security Manager will work closely with the Associate Director of Business Intelligence, and the Head of Information Governance (IG) & Data Protection Officer (DPO).

Caldicott Guardian

The Trust has appointed the Medical Director as the Caldicott Guardian.

The Caldicott Guardian is responsible for ensuring the confidentiality of patient confidential data and ensuring it is shared appropriately and securely.

Managers

Managers within every business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties. Managers must always contact the Head of IG & DPO if:

- they are unsure of the lawful basis which they are relying on to process personal data;
- they need to rely on consent for processing personal data;
- they need to prepare privacy notices or other transparency information they are unsure about the retention period;
- they are unsure on what basis to transfer personal data outside the European Economic Area (EEA);
- they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment;
- they plan to use personal data for purposes other than those for which it was originally collected;
- they plan to carry out activities involving automated processing including profiling or automated decision-making;

- they need help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors);
- they plan to share data with another organisation or person in a way which is new or could affect data subjects' rights.

All Staff

Everyone working for Leeds Community Healthcare or on behalf of Leeds Community Healthcare is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of personal data and support Leeds Community Healthcare in complying with data protection legislation, including undertaking Information Governance training on an annual basis.

5. GDPR Principles

The GDPR sets out the main principles for organisations when processing data. In accordance with Article 5 of the GDPR, the Trust must ensure that personal data is:

5.1 Lawfulness, Transparency and Fairness

Lawfulness

To process personal data and special category data lawfully, the Trust must identify a legal basis for each data processing activity.

An annual data mapping exercise is undertaken across the Trust which identifies all inbound and outbound flows of information and an appropriate condition under Article 6 and Article 9 of the GDPR is identified and documented.

Transparency and Fairness

General information about how we process personal data as a controller (referred to as "fair processing information") will be available on our website through privacy notices and other public-facing material.

5.2 Purpose Limitation

The Trust has clearly identified and documented the purposes for processing and included details of these purposes in our privacy information which we make available to both patients and our staff. All purposes are reviewed on an annual basis.

5.3 Data Minimisation

The Trust will only collect personal data required for specified purposes and ensure information we hold is periodically reviewed and removed when it is no longer required.

5.4 Accuracy

The Trust will take reasonable steps to ensure the accuracy of personal data and will carefully consider any challenges to the accuracy of information. This will be achieved by ensuring:

- appropriate processes are in place to check the accuracy of data;
- any mistakes are clearly identified as a mistake;
- all records will identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts;
- any challenges to the accuracy of personal data will be carefully considered when complying with an individual's right to rectification;

5.5 Storage limitation

We will ensure that personal data is not kept in an identifiable form for longer than is necessary. Due to our function as a public authority, the Trust retains some personal data for long periods of time.

Details of all of our retention and disposal periods are set out in our [Records Management Policy](#).

5.6 Appropriate Security

A key principle of the GDPR and Data Protection Act 2018 is that personal data must be processed securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'. This will be achieved by ensuring:

- A Network security policy (PL350) is in place and implemented across the Trust.
- Additional policies and controls are in place to enforce them.
- Information security risk shall be adequately managed and risk assessments on IT systems and business processes shall be performed where appropriate.
- The requirements for confidentiality, integrity and availability for the personal data we process are understood.
- Appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store the Trust information.
- Encryption and/or pseudonymisation are in place where it is appropriate to do so.
- Access to personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process.
- Regular testing is conducted and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Measures are implemented that adhere to an approved code of conduct or certification mechanism when necessary.
- All relevant information security requirements of the Trust shall be covered in agreements with any data processors, third-party partners or suppliers, and compliance against these is monitored.

6. Accountability

The Trust is **responsible** for complying with the GDPR and DPA18 and must be able to **demonstrate** compliance by evidencing the steps taken to comply. This will be achieved by ensuring:

- we take responsibility for complying with the GDPR and DPA 2018, at the highest management level and throughout our organisation;
- we keep evidence of the steps we take to comply with the GDPR and DPA 2018;
- appropriate technical and organisational measures are in place, which will be achieved by;
 - adopting and implementing data protection policies;
 - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
 - putting written contracts in place with organisations that process personal data on our behalf;
 - maintaining documentation of our processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out Data Protection Impact Assessments (DPIA) for uses of Personal Data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer;
 - adhering to relevant codes of conduct and signing up to certification schemes (where possible);
 - We review and update our accountability measures at appropriate intervals.

7. Lawful basis for processing

The Trust must determine the lawful basis for processing before starting any collection of personal data. The lawful basis for processing are set out in Article 6 of the GDPR and at least one of these must apply whenever Personal Data is processed:

- (a) Consent:** the individual has given clear consent to process their Personal Data for a specific purpose.
- (b) Contract:** the processing is necessary for a contract with the individual, or because they have asked the Trust to take specific steps before entering into a contract.
- (c) Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations).
- (d) Vital interests:** the processing is necessary to protect someone's life.

- (e) **Public task:** the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the Trust is processing data to perform its official functions).

In order to process **Special Categories Data**, the Trust must also ensure that one of the following applies:

- (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- (b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection;
- (c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) Processing relates to personal data which are manifestly made public by the data subject;
- (e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (f) Processing is necessary for reasons of substantial public interest, on the basis of EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (g) Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
- (h) Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

These conditions must be read alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

- Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2), (b), (g), (i) and (j).

- Schedule 1 Part 2 contains specific 'substantial public interest' conditions for Article 9(2)(h).

The Trust annually reviews the purposes of our processing activities, and selects and documents the most appropriate lawful basis for each activity to demonstrate compliance. This information is included in our privacy notices for both staff and patients.

8. Consent

Where relying on consent as the legal basis for lawful sharing of personal information, ensure the quality of consent meets new requirements and that:

- consent is active, and does not rely on silence, inactivity or pre-ticked boxes;
- consent to processing is distinguishable, clear, and is not "*bundled*" with other written agreements or declarations;
- data subjects are informed that they have the right to withdraw
- there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;
- separate consents are obtained for distinct processing operations; and
- consent is not relied on where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).

9. Individuals Rights

The Trust will respect individuals' rights when processing personal data. These are enshrined in the legislation as follows:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

The right to be informed is, however, a key right and applies in all circumstances (see Transparency and Fairness, section 5.1). The Trust has an Individuals Rights and Subject Access Request Procedure in place to support.

10. Data Processors and Contracts

Where it uses a data processor, the Trust is still responsible for data protection and liable for any data transferred.

The Trust is also liable for the Data Processor's compliance with the legislation and must only appoint processors who can provide sufficient guarantees that the requirements of the legislation will be met and the rights of data subjects protected. It must, therefore, ensure that there is an appropriate written contract with the data processor. The contract is important so that both parties understand their responsibilities and liabilities.

Contracts will set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller and which must, as a minimum set out the following:

- only act on the written instructions of the Trust;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the Trust and under a written contract;
- assist the Trust in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the Trust in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract;
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a Member State.

The Trust will apply the approach set out in the Procurement Policy Note (PPN03/17) Changes to Data Protection Legislation & General Data Protection Regulation, published by Crown Commercial Service.

11. Documentation

The Trust is required to maintain a record of its processing activities, covering areas such as processing purposes, data sharing and retention.

A Data Mapping review of all data processing activities across the Trust will be undertaken on an annual basis facilitated by the Information Governance team. The review will identify all inbound and outbound flows of personal identifiable information from each department and Business Unit, the purposes of the flow, what type of personal data is involved, who it is shared with, the lawful basis and whether an information sharing agreement has been established.

12. Data Protection by Design and Default

The Trust will ensure that privacy and data protection issues are considered at the design phase of any new system, service, product or process and that appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights are in place. This will involve but not limited to;

- Only using Data Processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- Anticipating risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- Making data protection an essential component of the core functionality of our processing systems and services.

13. Data Privacy Impact Assessment (DPIA)

The GDPR introduces a new obligation to carry out a DPIA before carrying out types of processing likely to result in high risk to individuals' interests.

The Trust will consider if a full DPIA is necessary if the processing of personal data involves:

- evaluation or scoring (including profiling and predicting)
- automated decision making
- systematic monitoring of data subjects, including in a publicly accessible area
- sensitive data (special categories of data as defined in Article 9 and data regarding criminal offences)
- data being processed on a large scale
- matched or combined datasets
- vulnerable individuals
- transferring data outside the European Union
- innovative technical or organisational solutions
- preventing data subjects from exercising a right or using a service or a contract

As a minimum, a DPIA will include;

- A description of the envisaged processing operations and the purposes of the processing;
- An assessment of :
 - (i) the need for and proportionality of the processing and
 - (ii) the risks to data subjects (as viewed from the perspective of data subjects) arising; and
- A list of the measures envisaged to mitigate those risks and ensure compliance with the GDPR.

13. Data Protection Officer

The GDPR introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

The Trust's DPO is Narissa Leyland, who can be contacted via email dpo.lch@nhs.net or phone: 0113 220 8572

Or at the following address:
Information Governance Team
Leeds Community Healthcare
Stockdale House
Victoria Road
Leeds
LS6 1PF

14. Personal Data Breaches

It is a legal obligation to notify personal data breaches of the GDPR under Article 33 within 72 hours, to the ICO, unless it is unlikely to result in a risk to the rights and freedoms of individuals. Article 34 also makes it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms. It is also a contractual requirement of the standard NHS contract to notify incidents in accordance with this guidance. By notification, this may be an initial summary with very little detail known at the outset but a fuller report that might follow. There is no expectation that a full investigation will be carried out within 72 hours.

The Trusts documents all data breaches even if they don't need to be reported to the Information Commissioner.

The '[Guide to the Notification of Data Security and Protection Incidents](#)' must be followed when a data breach has been detected. The guidance applies to all organisations operating in the health and social care sector. This guidance has been incorporated into the Personal Data Breach Management Procedure, which is aligned to the Incident & Serious Incident Policy.

15. International Transfers

Current data protection laws impose restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

16. Monitoring Compliance and Effectiveness

Minimum requirement to be monitored / audited	Process for monitoring / audit	Lead for the monitoring/audit process	Frequency of monitoring / auditing	Lead for reviewing results	Lead for developing / reviewing action plan	Lead for monitoring action plan
Compliance with the Data Security & Protection Toolkit	Reporting to the IG Group	Head of Information Governance & Data Protection Officer	Quarterly	Director of Finance and Resources	Head of Information Governance & Data Protection Officer	IG Group
Annual Information Governance Audit	Reporting to the Audit Committee	Head of Information Governance & Data Protection Officer	Annually	Director of Finance and Resources	Head of Information Governance & Data Protection Officer	IG Group

17. Training needs

All staff must adhere to the IG training requirements set out in the Trust's Mandatory and Statutory Training Policy.

18. Approval and Ratification process

The policy has been approved by the IG Group, Clinical and Corporate Policy Group and ratified by SMT on behalf of the Board with oversight of the Audit Committee.

19. Dissemination and Implementation

Dissemination of this policy will be via the Clinical and Corporate Policy Group/Work force policies to services and made available to staff via the IG intranet page.

20. Review arrangements

This policy will be reviewed in three years by the author or sooner if there is a local or national requirement then ratified by the SMT with oversight of the Audit Committee.

21. Associated documents

The policies / procedures in place to support the IG Framework are:-

Confidentiality Code of Conduct – PL306
Records Management Policy – PL235
FOI Procedure – IG004
Individual Rights and Subject Access Request Procedure – IG003
Information Handling Guideline – GL083
Network Security Policy – PL350
Data Protection Impact Assessment Policy – PL374
Data Protection Impact Assessment Procedure – IG002
Data Breach Management Procedure - IG-005
Information Asset Procedure - IG-001

22. References

[General Data Protection Regulation 2018](#)
[Data Protection Act 2018](#)
[Human Rights Act 1998](#)
[Privacy and Electronic Communications Regulations 2003](#)

[A Manual for Caldicott Guardians \(2017\)](#)

[Department of Health, Confidentiality: NHS Code of Practice \(2003\)](#)

[Department of Health, Information: To Share or Not to Share \(2013\) \(Caldicott 2\)](#)

[Report on the Review of Patient-Identifiable Information \(1997\) \(The Caldicott Report\)](#)

[NHS Digital, Code of Practice on Confidential Information \(2014\)](#)

Policy Consultation Process

Title of Document	Data Protection Policy
Author (s)	Narissa Leyland – Head of IG& DPO
New / Revised Document	New
Lists of persons involved in developing the policy	Narissa Leyland
List of persons involved in the consultation process	Richard Slough Assistant Director of Business Intelligence Catherine Duff Interim Quality Lead for Children's Business Unit Jo Sykes Clinical Advisor & Clinical Safety Officer Rob Arnold Deputy Medical Director

Appendix: 2 – Authors Guide for writing/Review and Approval of Procedural Documents

	Title of new/reviewed Document	Yes/No/Unsure	Comments
1. TITLE			
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2. RATIONALE			
	Are there defined reasons for document development?	Yes	
3. REVIEW PROCESS			
	Is the method described in brief?	Yes	
	Are individuals involved in the development identified?	Yes	
	Has a rational attempt been made to ensure the relevant expertise has been used?	Yes	
	Is there evidence of a consultation with stakeholders and users?	Yes	
4. CONTENT			
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5. EVIDENCE BASE			
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are all supporting documents referenced?	Yes	
6. APPROVAL			
	Has the named Director had sight of the document?	Yes	IG Group approved the policy
	Does the document identify which committee/group will approve it?	Yes	
	If applicable have the joint Human Resources/staff side committee (or equivalent) approved the document?	n/a	
7. DISSEMINATION and IMPLEMENTATION			
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8. DOCUMENT CONTROL			
	Does the document identify where it will be		

	held?		
	Have archiving arrangements for superseded documents being addressed?		
9.	PROCESS to MONITOR COMPLIANCE and EFFECTIVENESS		
	Are there measurable standards or KPI's to support the monitoring compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	REVIEW DATE		
	Is the review date identified?	Yes	
	Is the frequency identified? Recommend every 2/3 years or sooner if required.	Yes	
	Is this an acceptable time frame?	Yes	
11.	OVERALL RESPONSIBILITY for the DOCUMENT		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes	
12.	FORMAT and CONTENT		
	Arial font	Yes	
	Font size 12	Yes	
	Trust Logo on front page	Yes	
	Title of policy on front page	Yes	
	Policy control page completed		
	Is this a review of an existing document, if so have all changes/amendments been recorded in the table provided	No	
	Footer of each page details: name of policy, author and date of publication	Yes	
	Numbered sequentially	Yes	
	Appendices present (where required)	None	
	Impact assessment carried out	Yes	
	Glossary included as appropriate	Yes	
	Proof read the document	Yes	
Author			
If you are satisfied and want to approve this document please sign and date it			
NAME	Narissa Leyland	DATE	
SIGNATURE			
FINAL APPROVAL			