Confidentiality and Data Protection Policy

Printed copies must not be considered the definitive version

DOCUMENT CONTROL	**POLICY NO.**	IG - 102	
Policy Group:	Information Assurance and Security		
Lead Author:	Head of Information Governance		
Lead Executive:	Medical Director/SIRO		
Scope:	Board wide	**Version no.**	5.0
Status:	Approved	**Implementation date:**	August 2013
Last review date:	October 2025	**Next review date**	October 2028
Approved by:	Board Management Team	**Approval date:**	November 2025
Equality Impact Assessed:	Yes	**Equality Impact Assessment date:**	September 2025
Data Protection Impact Assessed:	Not required	**Data Protection Impact Assessment Date:**	Screening questionnaire completed September 2025

Policy on a page

Summary & Aim	Key Requirements
To ensure NHS Dumfries & Galloway meets its legal obligations as a data controller in maintaining the confidentiality of the personal information it processes for its staff and patients. Current relevant legislation, which forms the basis of this policy, are DPA18 and UKGDPR	• Awareness of, and adherence to, the 6 data protection principles and the Caldicott principles for all personal data processing • Demonstrating accountability, as a data controller, for all personal data processing • Promoting transparency within NHS Dumfries & Galloway in how staff and patient information is captured, processed, retained, shared, archived and destroyed
Target Audience	**Previous Names**
• All employees, bank workers, agency staff, contractors, students, volunteers etc	• Data Protection Policy

Equality and Diversity Statement
NHS Dumfries and Galloway recognise that some communities within society are more likely than others to experience discrimination, prejudice and inequalities. The Equality Act 2010 specifically recognises the protected characteristics of **age, disability, sex, race, religion or belief, sexual orientation, gender reassignment, pregnancy and maternity, and marriage and civil partnership**. The Fairer Scotland Duty, also requires NHS Dumfries and Galloway to actively consider how socio-economic disadvantage can be reduced when making strategic decisions. The New Armed Forces Covenant Statutory Duty places an expectation on NHS Dumfries and Galloway to consciously consider the Armed forces Covenant when developing, delivering and reviewing policies and decisions which may impact the Armed Forces community and help improve their access to public services. Consideration on all of the protected characteristics, the Fairer Scotland Duty and the Armed Forces Covenant are included within the Equality Impact Assessment process and documentation, which must be completed as part of the Policy Development Process. NHS Dumfries and Galloway is committed to promoting and advancing equality, removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those who do not. This applies both in the provision of services and as our role as a major employer. NHS Dumfries and Galloway believe that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discrimination practice.

CONTENTS

1. PURPOSE AND RATIONALE

1.1 Confidentiality is a fundamental principle in the delivery of health care services. The personal information collected and processed by NHS Dumfries & Galloway relates to staff and patients. This data must be treated with care and respect to secure its integrity, protect it from inappropriate disclosure or access and ensure it is readily available to authorised staff when required.

1.2 NHS Dumfries & Galloway will maintain the confidentiality of the information it holds by adhering to legislated requirements, professional codes of practice and conduct and NHS Dumfries & Galloway policies and procedures.

2. POLICY AIMS

2.1 This policy explains how NHS Dumfries & Galloway meets its legal obligations and NHS standards relating to the confidentiality and security of information. The requirements outlined in this policy will be supplemented by other documentation which will provide detailed information on specific subject areas.

2.2 The requirements outlined in this policy are primarily based on the UK General Data Protection Regulation (UKGDPR). The which is supplemented by the Data Protection Act 2018. However, other relevant legislation and guidance may be referenced, including other data protection laws.

2.3 NHS Dumfries & Galloway endorse the seven UKGDPR principles and all staff who process personal information must follow these principles in that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Only processed for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary for the intended purpose
- Accurate and kept up to date
- Kept in a way which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and only for as long as necessary; and
- Processed in a way which ensures it is kept secure

The seventh data protection principle, known as the Accountability principle, requires NHS Dumfries & Galloway to take responsibility for what it does with personal data and how it complies with the other principles.

UKGDPR NHS Dumfries & Galloway will ensure that all staff have the knowledge and tools required to meet its legal obligations including appropriate Data Protection training, staff communications and relevant policies and procedures.

NHS Dumfries & Galloway is committed to adhering to the Caldicott principles when handling patient identifiable data. These principles are:

- Justify the purpose(s)
- Use personal data only when absolutely necessary
- Use only the minimum amount of personal data necessary to satisfy your purpose
- Access to personal data should be on a strict need-to know basis
- Everyone who has access to personal data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality
- Inform patients and service users how their personal information is used

3. POLICY SCOPE

3.1 This policy applies to all staff employed by NHS Dumfries & Galloway. In addition, it is also applicable to all contractors, partnership organisations, students and visitors not directly employed by NHS Dumfries & Galloway but engaged to work with, or have access to, information for which NHS Dumfries & Galloway is the data controller.

4. DEFINITIONS

4.1 **Data Protection Act 2018** (DPA18) controls how personal information is used by organisations, businesses or the government. **UK General Data Protection Regulation** (UKGDPR) is a regulation in domestic law on data protection and privacy for all living citizens of the UK.

4.2 **Data Protection Officer** (DPO) required by NHS Dumfries & Galloway, under UKGDPR, to ensure the organisation applies the laws protecting the personal data of its patients and staff.

4.3 **Personal data/information** is information that relates to an identified or identifiable individual.

4.4 **Special category data/information** is personal data that requires more protection as it is sensitive. Specifically this type of data relates to an individual's racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, *health data* and sexual orientation. Data relating to criminal convictions is not special category data, but additional rules and safeguards exist for the processing of this information due to the associated risks.

4.5 **Data Controller** NHS Dumfries & Galloway, as an organisation, is a data controller as we determine what information we process and why.

4.6 **Data Processor** is any person(s) or organisation, other than an employee of the organisation, who processes data on behalf of the controller.

4.7 **Processing** refers to the collection, recording, storage, usage, analysis, combining, disclosure and deletion of data.

4.8 **Staff** refers to all employees, bank workers, agency staff, contractors, students, volunteers etc

5. DUTIES / RESPONSIBILITIES

5.1 All employees of NHS Dumfries & Galloway are bound by a legal duty of confidentiality to protect and keep up to date personal information they access during the course of their work. This is both a legal and contractual responsibility and a requirement under the common law duty of confidence.

5.2 In order to ensure that both new and current staff are aware of their responsibilities regarding confidentiality and data protection NHS Dumfries & Galloway will provide a mandatory training and awareness which staff must be compliant with.

5.3 Personal data, may be held in a number of formats including paper, on electronic system etc and, is considered to be any information which, either directly or indirectly, identifies an individual, e.g. name, address, email address, CHI number, employee number etc.

5.4 With respect to personal data, all staff must ensure that:

- It is effectively protected against improper disclosure when it is received, used, stored, transferred or disposed of.
- Access to the data is on a need-to-know basis. Access can be for clinical treatment, patient administration purposes or operational purposes such as an IT professional needing to access personal data to resolve system issues or errors.
- Information contained in staff and patient records is accurate and up to date.
- Disclosure is limited to the purpose for which it is required, and any can be appropriately justified either under data protection or other relevant legislation.
- All data breaches must be reported in accordance with NHS Dumfries & Galloway Personal Data Breach Recording Procedure, and an incident raised on InPhase. All issues concerning confidentiality are referred to the Data Protection Officer in a timely manner.
- Confidential data is disposed of correctly in line with current retention policy timescales. Please refer to the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2024.

5.5 Chief Executive

As the Accountable Officer for NHS Dumfries & Galloway, the Chief Executive has overall responsibility for Data Protection, which is delegated to the Caldicott Guardian and Senior Information Risk Owner (SIRO) to manage.

5.6 Medical Director

- The Medical Director has executive responsibility for Information Assurance and Security Planning.

- The Medical Director has responsibility for ensuring that Information Assurance and Security Planning is adequately and appropriately resourced to complete its function.

5.7 Senior Information Risk Owner (SIRO)

The role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Board and provide written advice to the Chief Executive on the content of their annual governance statement in regard to information risk. This role in NHS Dumfries & Galloway is currently fulfilled by the Medical Director.

5.8 Caldicott Guardian

The Caldicott Guardian is responsible and accountable for protecting the confidentiality of our patients' health and care information, ensuring it is used ethically, legally, and appropriately. This role in NHS Dumfries & Galloway is currently fulfilled by the Medical Director.

5.9 Information Assurance Committee

NHS Dumfries & Galloway Information Assurance Committee (IAC) has the responsibility to:

- Monitor compliance with legislation.
- Monitor compliance with local policies, procedures and guidance.
- Review and approve all information governance procedures.
- Review all information governance policies prior to approval by Board Management Team

5.10 Data Protection Officer (DPO)

The appointment of a DPO for an organisation such as NHS Dumfries & Galloway is a mandatory requirement of the UKGDPR.

The DPO is responsible for ensuring NHS Dumfries & Galloway and its staff are kept informed and given advice, guidance and support to meet the obligations of the organisation as required by data protection legislation.

The DPO is responsible for monitoring compliance with UKGDPR and how it relates to the personal information processed by NHS Dumfries & Galloway, including the management of internal data protection activities, providing

advice on data protection impact assessments, training staff and conducting internal audits.

The DPO is the first point of contact for the Information Commissioner's Office (ICO) and for individuals (employees, patients etc) whose personal information is processed by the organisation.

This role in NHS Dumfries & Galloway is currently fulfilled by the Head of Information Governance.

5.11 Head of Information Governance

The Head of Information Governance is responsible for:

- The implementation and enforcement of all Information Governance Policies, Procedures and guidelines
- Providing assistance and guidance in the production of all required information governance documentation including Data Protection Impact Assessments (DPIA), Data Processing Agreements (DPA) and Information Sharing Agreements (ISA)
- Developing, maintaining, reviewing and enforcing procedures to ensure the confidentiality of data
- Ensuring compliance with all relevant legislation and specific NHS Scotland Information Governance guidance
- Developing Information Governance (IG) awareness training material to ensure that all staff are aware of their data protection responsibilities.
- Provide additional training and awareness sessions when any training needs are identified.
- Monitoring, recording, investigating and reporting actual or potential data breaches.
- Presenting reports to the Information Assurance Committee covering such items as:
    - Complaints and breaches reported to the Information Commissioner's Office (ICO)
    - Incidents reported (InPhase)
    - User access reports (Fairwarning)
    - Emerging data protection or information risks

5.12 Directors and Managers

All NHS Dumfries & Galloway directors and managers are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is continual compliance.

5.13 All Staff

Protecting and maintaining the confidentiality of all personal information is a mandatory requirement for all staff. All staff must adhere to the NHS Scotland Code of Practice: Protecting Patient Confidentiality.

All staff have a confidentiality clause included in their contract of employment. Staff are required to comply with all NHS Dumfries & Galloway policies and procedures relating to confidentiality and data protection matters at all times. Mandatory Information Governance and Cyber Security training modules must be completed by all staff, at induction to the organisation and every year thereafter, for the duration of their employment with the board.

User access to clinical systems is continually monitored and any detected, or suspected, instances of inappropriate access by staff will be investigated. This could result in formal disciplinary action being taken.

Please refer to Fairwarning - Staff Guide and Fairwarning - Manager Guide for further information.

6. PROCESS / PROCEDURES

6.1 Data Protection Impact Assessment (Article 35 – UKGDPR)

A Data Protection Impact Assessment is a legal requirement under Article 35 of UKGDPR and is an assessment tool used to identify, assess and mitigate any actual or potential risks to confidentiality which may arise from a proposed or existing process or project involving the use of personal data which is classed as high risk processing. Completing a DPIA:

- helps identify the most effective ways to comply with data protection obligations,
- ensures NHS Dumfries & Galloway meets the expectations of its staff and patients with regards to protecting the confidentiality of their information and
- demonstrates accountability for the use of personal data.

The DPIA allows services, departments and individuals to identify and resolve problems at an early stage, reducing information risks, associated costs and reputational damage which may otherwise occur.

Failure to manage confidentiality risks can result in enforcement action by the Information Commissioner's Officer (ICO), including substantial fines. The DPIA is one specific aspect of risk management which feeds into the overall risk management processes of our organisation.

To ensure ongoing compliance with DPA18, UKGDPR and Network and Information Systems Directive (NIS), NHS Dumfries & Galloway must follow due diligence when using personal information.

6.2 Information Sharing Agreements (ISA)

NHS Dumfries & Galloway has Information Sharing Agreements in place where necessary to support lawful sharing of personal and special category data with other organisations and agencies.

These agreements provide staff with detailed and specific guidance on the appropriate sharing of information between the relevant parties.

To ensure information is shared appropriately with other parties where an ISA **is not required or appropriate**, staff must be satisfied that there is a legal basis for the requesting party to access this information prior to releasing it. Staff must consider how much confidential information it is necessary to share before disclosure in order to provide the minimum amount of confidential information required for the intended purpose.

Information can be disclosed when:

- required by law or under a court order with appropriate authorisation as described in the Data Protection Act 2018
- it is necessary for the prevention and detection of serious crime with appropriate authorisation as described in the Data Protection Act 2018
- it is in the public interest, such as concerns about a child or vulnerable adult.
- the individual has provided explicit written consent.

The list is not exhaustive, and further advice can be sought from the Information Governance Team.

6.3 Subject Access Requests (Article 15 –UKGDPR)

The UKGDPR provides data subjects with the right of access to their own personal data as processed by NHS Dumfries & Galloway. Requests are submitted to NHS Dumfries & Galloway by contacting the Data Protection Team. Subject Access Request forms are available on both nhsdg.co.uk and the intranet, or by contacting the team at dg.dpa-office@nhs.scot

A data subject is under no obligation to complete any pre-determined request form in order to obtain a copy of their personal data and requests can be made by email, social media or by phone. Proof of ID must always be requested and validated before any personal data is released.

The UKGDPR allows one calendar month for organisations to respond to a Subject Access Request. If this is not possible then the requestor must be informed.

Subject Access Requests will be processed by NHS Dumfries & Galloway in compliance with UKGDPR, Data Protection Act 2018 and Data Use and Access Act 2025.

More information about Subject Access Requests can be found in NHS Dumfries & Galloway Subject Access Request Procedure available on the intranet.

6.4 Accidental Disclosure

Staff have a legal duty of confidentiality to keep personal data safe and not divulge personal information unless appropriate. Inappropriate disclosures can be as a result of a lack of attention or awareness e.g.

- conducting conversations about a patient or a colleague in public places
- lack of diligence when sending mail or emails to ensure they are properly addressed to the intended recipient.
- leaving a device logged on and unlocked when unattended.
- documents being left behind in meeting rooms or not collected promptly from printers.

Staff are reminded that they may be held personally liable for a breach of personal data.

Staff should also be aware that significant financial penalties can be imposed on NHS Dumfries & Galloway under data protection legislation for serious breaches of personal data.

All instances of accidental disclosure must be reported in accordance with the NHS Dumfries & Galloway Personal Data Breach Notification Procedure. More information is provided in 6.5 Data Breach Reporting.

6.5 Data Breach Reporting

All breaches of personal data which are discovered by NHS Dumfries & Galloway employees, agency staff, contractors, students and volunteers must be reported immediately by raising an incident on InPhase. On discovery of a personal data breach the following steps must be taken:

Step 1. The data breach must be reported on InPhase without delay, recording the full details of the data breach Create new NHSDG Adverse Events

Step 2. Your line manager and the Information Governance Team must be informed that a breach of personal data has occurred. Advice must be sought without delay from the Information Governance Team to determine whether the data subject should be advised that their personal data has been breached. This will be dependent on the nature of the breach, the information disclosed and if notifying the data subject is likely to cause serious harm to their physical or mental wellbeing.
dg.dataprotection@nhs.scot

Step 3. If appropriate, contact data subject to advice of data breach. This contact should be made by the service/department responsible for the breach.

Step 4. Consider any measures which can be taken to contain the breach or prevent it from becoming more serious.

The Information Governance Team will support the investigation of the data breach as required and assist with any further action necessary as described in the NHS Dumfries & Galloway Personal Data Breach Notification Procedure.

6.6 The Freedom of Information (Scotland) Act 2002 (FOISA)

This legislation provides individuals with the right to request, and be given, information from a wide range of public organisations including NHS Dumfries & Galloway.

There are restrictions on the type of information that may be released under FOISA.

For more information, please refer to NHS Dumfries & Galloway Freedom of Information Policy.

6.7 Counter Fraud Services

NHS Dumfries & Galloway has a signed Partnership Agreement with NSS Counter Fraud Services (CFS) which covers the roles and responsibilities of both parties in relation to the use of shared personal data for fraud investigations.

NHS Dumfries & Galloway is also required by Audit Scotland to take part in the National Fraud Initiative, a data matching exercise intended to deter and detect possible cases of fraud. NHS Dumfries & Galloway is required to provide key payroll data to allow comparison to be made with data provided by other public bodies.

The processing of data by Audit Scotland (or by the Cabinet Office on behalf of Audit Scotland) in data matching exercises is carried out under Part 2A of the Public Finance and Accountability (Scotland) Act 2000. It does not require the consent of the individuals concerned, as detailed in the Data Protection Act 2018, as there is an overarching legal requirement. Data matching performed by Audit Scotland is subject to the Audit Scotland Code of Data Matching Practice.

6.8 Working Offsite

Staff are often required, or choose, to work from another location, in the community or from home and may need to take confidential information with them. Staff should be aware that:

- taking home/removing paper documents which contain personal information is discouraged unless absolutely necessary and should be discussed in advance with a line manager.
- compliance with all NHS Dumfries & Galloway policies and procedures is still required whether working at your recognised base, another location, in the community or from home. Confidential personal data must be stored securely when not being used.

- work related personal data must never be forwarded to a staff member's personal email account. work related personal data must never be transferred to or stored on a privately owned device e.g. PC, laptop, tablet, mobile phone, removable media mobile devices such as laptops, tablets and mobile phones should always have the screen locked when not in use.
- if using a mobile device in any public space (such as in the hospital canteen, a café or during a train journey) care must be taken at all times to prevent other people being able to view the content on the screen.

6.9 Abuse of Privilege

Staff are entrusted with access to sensitive personal information about patients and colleagues. This access is a privilege which comes with a legal and ethical responsibility to uphold confidentiality at all times.

Accessing patient or staff records without a clear, work-related need is a serious breach of trust and an abuse of that privilege. It is also an offence under data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

All staff must ensure that personal data is only accessed when necessary for the delivery of care or the performance of official duties. Unauthorised access—whether out of curiosity, personal interest, or any other non-professional reason—is strictly prohibited and may result in:

- **Disciplinary action**, up to and including dismissal
- **Referral to professional regulatory bodies**
- **Criminal investigation and prosecution**

Protecting confidentiality is fundamental to maintaining public trust in the NHS. If you are ever unsure about whether access is appropriate, seek guidance from your line manager or your organisation's Information Governance team

6.10 Monitoring

The effectiveness of this policy will be monitored by the Information Assurance Committee on a quarterly basis using input from the following sources:

- data breaches reported via InPhase or directly to the Information Governance Team
- Fairwarning reports
- complaints relating to personal data processed by NHS Dumfries & Galloway
- complaints to the ICO regarding NHS Dumfries & Galloway's use of personal data, breaches of confidentiality, unnecessary processing, etc.

7 CONSULTATION

7.1 Consultation on the Confidentiality and Data Protection Policy was led by the Lead Author and included:

- Information Assurance Committee
- Cyber Security Team
- SIRO/ Caldicott Guardian/ Medical Director
- Board Management Team
- Data Protection Officer
- Equality & Diversity Lead
- Staff side representative
- Health & Social Care Partnership Management Team
- Area Partnership Forum

8 TRAINING AND SUPPORT

8.1 All NHS Dumfries & Galloway employees, bank workers, agency staff, contractors, students, volunteers or anyone who processes information for which NHS Dumfries & Galloway is the data controller must be compliant with the annual Information Governance & Cyber Security training requirement.

8.2 Training and awareness sessions on confidentiality and data protection are available, on request, from the Information Governance Team at dg.dataprotection@nhs.scot

8.3 Should anyone require further assistance or support on any of the processes or procedures set out in this policy they can contact the Information Governance Team at dg.dataprotection@nhs.scot

9 MONITORING

9.1 The monitoring arrangements for this Policy are set out in the table below.

Element to be monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Compliance with legislation (DPA18/UKGDPR)	Review of InPhase incidents, ICO reports, complaints	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Compliance with local policies, procedures, guidelines	Review of Fairwarning reports, InPhase incidents, ICO reports, complaints	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly

Element to be	Monitoring	Reporting		
Data Breaches (incl. inappropriate access)	InPhase	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Compliance with mandatory IG/Cyber Security training requirement	LearnPro reports	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	3 monthly
Completion of required IG/IS documentation	Review of registers: DPIAs, ISAs, DPAs, SSPs	Head of Information Governance	Information Assurance Committee	3 monthly
			Audit & Risk Committee	

10 EQUALITY IMPACT ASSESSMENT

10.1 An Equality Impact Assessment was completed on 05/09/2025. The completion of an EIA will be considered during each subsequent review of this policy.

11 DATA PROTECTION IMPACT ASSESSMENT

11.1 A Data Protection Impact Assessment (DPIA) is not required for this policy, as determined following completion of the screening questionnaire on 04/09/2025.

12. DOCUMENT CONTROL SHEET

12.1 Document Amendment History

Version	Section(s)	Reason for update
0.1	NHS Lanarkshire exemplar document	Editing required for NHS Dumfries & Galloway purposes
1.0	ALL	1st draft
1.1	ALL	2nd draft
1.2	ALL	Final draft following review and amendments as recommended by the Information Assurance Committee – Key Points added.
1.3	ALL	Final recommendation for approval by APF
1.4	ALL	Updates for Public Records (Scotland) Act 2011
2.0	ALL	Updates for SG Information Security Framework DL2015/17
3.0	ALL	Document rewritten to incorporate changes required by UKGDPR/DPA18. Title changed to make it easier to find on NHSDG intranet. Reduced detailed content now available in separate subject specific documents
4.0	ALL	Transferred to new policy document template approved March 2022, reviewed in accordance and with reference to Policy Management Policy reviewed January 2022, and Document Development checklist. Includes references to approved data breach/SAR procedures.
5.0	ALL	Pg 2 Updated Equality & Diversity statement Reviewed all sections and updated as required including updates to legislation, internal policies/procedures and systems. Pg 13 Expansion of Section 6.9 Abuse of Privilege

12.2 Distribution

Name	Responsibility	Version number
Corporate Business Manager	Update Policy Register	5.0
Information Assurance Committee	For comment	5.0
Board Management Team (BMT)	For approval	5.0
Information Governance Team	To place on intranet and monitor policy compliance	5.0
Communications	Place in ‘latest news’	5.0

12.3 Associated documents

NHS Dumfries & Galloway Information Security Policy
NHS Dumfries & Galloway Information Assurance Strategy
NHS Dumfries & Galloway Computer Usage Policy
NHS Dumfries & Galloway Personal Data Breach Notification Procedure
NHS Dumfries & Galloway Subject Access Request Procedure
NHS Dumfries & Galloway Freedom of Information Policy
Audit Scotland Code of Data Sharing Practice
NHS Scotland Counter Fraud Services – Partnership Agreement with Health Boards 2019-2022

12.4 Action Plan for Implementation

Action	Lead Officer	Timeframe
Update policy register	Corporate Business Manager	Immediate
Place in 'latest' news	Communications	Immediate
Place on internet nhsdg.co.uk	CBS Team	Immediate
Dissemination to all staff through line management	General Managers	Continual availability of policy document on nhsdg.co.uk