South Warwickshire
NHS Foundation Trust

Information Governance

SWH 00346
Information Governance Policy
Incorporating Data Protection and Confidentiality

The Trust's Intranet holds the current approved guidance documents.

Notice to staff using a paper copy of this document.
Staff must ensure that they are using the most up-to-date document to guide their practice and must check that the version number of the paper copy matches that of the one on the Intranet.

Version	V3.0
Job Title of Responsible Manager	Information Governance Group
Replacing Document	SWH 00346 Information Governance Policy V2.1 SWH 00181 Confidentiality Code of Practice V4.0 SWH 00323 Data Protection Policy V4.0 SWH 00198 Transmission of Confidential Data Policy V2.0
Ratifying 'Body'	Policy Review Group
Date Ratified	August 2020
Date for Review	August 2025
Relevant Standards:	Health and Social Care Act 2008 (Regulated Activities) [Amendment] Regulations 2015: 17

Document History

Issue Status e.g. Draft or Final	Catalogue and Version Number	Document Title	Date	Actioned by: (Job Title)	Page/ Section/ Paragraph	Comments
Final	SWH 00346 V1.0	Information Governance Policy	April 2010	Policy Review Group	Whole Document	Ratified Document
Final	SWH 00346 V1.1	Information Governance Policy	February 2013	Policy Review Group	Whole Document	Ratified Document
Draft	SWH 00346 V1.2	Information Governance Policy	March 2015	Information Governance Manager	Page 5, para. 3	Reference to disciplinary proceedings for breaches against the Data Protection Act 1998 and/or the Trust's Information Governance Policy
Final	SWH 00346 V2.0	Information Governance Policy	August 2017	Policy Review Group	Whole document	Ratified document
Final	SWH 00346 V2.0	Information Governance Policy	November 2019	Information Governance & Security Steering Group	Whole document	Changes to whole document to reflect 2018 legislation.
Draft	SWH 00346 V3.0	Information Governance Policy Incorporating Data Protection and Confidentiality	June 2020	Information Governance & Security Steering Group	Whole document	Four closely related documents merged: Information Governance policy, Confidentiality Code of Practice, Data protection policy and Transmission of Confidential data policy. Updated to refer to 2018 legislation
Final	SWH 00346 V3.0	Information Governance Policy Incorporating Data Protection and Confidentiality	August 2020	Policy Review Group	Whole document	Ratified document

Table of Contents

To access a section directly from the Table of Contents – 'hover' the mouse over the section you require and then press Ctrl and click the mouse.

1 Frequently Asked Questions

To help with navigation of this document, frequently asked questions are listed below, with hyperlinks to the relevant section.

- I work closely with my colleague; can we share each other's passwords? No
- What is the guidance on USBs and other removable media?
- Can I store identifiable information on my desktop? No
- Do I have a right to look at my own records, or those of family or friends? No
- How do I obtain a copy of my records?
- How should I secure information?
- What is a clear desk approach?
- How should I transport paperwork?
- What is the guidance on post?
- How should I securely email?
- Can I access my work email on my personal phone? Yes, you need to apply to IT
- Can I use WhatsApp? Yes, if you follow the guidance
- Can I send a fax?
- What is the guidance around verbal confidentiality?
- Can I speak to a patient's relatives?
- Can I speak to the police or social workers about a patient?
- Can I leave a message?
- I've been asked to disclose some confidential information and I'm not sure what to do.
- I've been asked to disclose confidential information and I'm still not sure what to do.
- How often should I complete Information Governance training? Annually
- What are the Data Protection Principles?
- What are the Caldicott Principles?
- What is a privacy notice?
- What is the definition of consent?

This is not an exhaustive list of questions that staff may have, and all staff should be familiar with the contents of this policy.

2 Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources; it plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance to ensure that information is effectively managed, and that appropriate

policies, procedures and management accountability structures are in place and provides a robust framework for Information Governance (IG).

This policy gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. The Trust will establish and deploy a series of IG policies, supported by procedures, standards or guidelines to ensure its information is secure and managed in accordance with all relevant legislation and standards.

The NHS cannot operate effectively if the patients we need to treat do not trust us to provide confidential and effective care. Part of this trust is being able to provide confidential information to clinicians and other staff and be confident that it will remain confidential and only be shared when necessary.

The Data Protection Act (2018) and the General Data Protection Regulation sets the legal framework, by which we can process personal information. It applies to information that might identify any living person.

The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential.

The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A).

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

3 Purpose

This document provides guidance for everyone on processing information in accordance with the principles and legal obligations outlined in the Data Protection Act (2018), General Data Protection Regulation and common law duty of confidentiality. It explains how we can comply with best practice for information handling within the NHS as described in the NHS Code of Confidentiality, Data Security and Protection Toolkit and the Caldicott Reports.

Personal data may belong to current, past and prospective patients, current, past and prospective employees, suppliers, contractors and business partners.

Personal data may be paper based or electronic. It includes but is not limited to:

- All patient information including health records
- Personnel records which include those held by line managers and those held centrally by the Human Resources department
- CCTV videos and other audio/visual recordings
- Photographs, x-rays and other images
- Emails

- Computer disks, tapes, CD ROMs, and other electronic media

The objectives of this policy are to:

- Demonstrate the ways in which we ensure that patient and staff data is handled effectively and securely
- Promote best practice and innovative use of personal information
- Ensure that all staff understand their responsibilities and obligations

4 Audience

This policy applies to all staff, contractors and their sub-contractors and volunteers including support organisations; anyone who is involved in handling patient, staff or other personal information.

5 Associated Trust Documents

SWH 00020	Incident Management Policy including the Management of Serious Incidents
SWH 00356	Being Open and the Duty of Candour
SWH 00422	Access to Health Records Policy
SWH 00519	Email Usage Policy
SWH 00384	Freedom of Information Act Policy
SWH 00319	Information Governance Accreditation and Privacy by Design Policy
SWH 00530	Information Security Policy
SWH 01626	Internet Usage Policy
SWH 00848	Pseudonymisation Policy
SWH 04360	National Data Opt Out Policy
SWH 04355	Unauthorised Access to Data Procedure
SWH 00007	Information Data Quality Assurance Policy
SWH 00169	Management of Healthcare Waste Policy
SWH 00168	Medical Devices Policy
SWH 04359	Photography and Recording Policy

6 Responsibilities/Duties

6.1 Board of Directors (BoD)

The BoD is responsible for determining the governance arrangements of the Trust including effective risk management processes. It is responsible for ensuring that the necessary clinical policies, procedures and guidelines are in place to safeguard patients and reduce risk. In addition, they will require assurance that clinical policies, procedures and guidelines are being implemented and monitored for effectiveness and compliance.

6.2 Chief Executive

The Chief Executive Officer (CEO) has overall responsibility for patient safety and ensuring that there are effective risk management processes within the Trust which meet all statutory requirements and adhere to guidance issued by the Department of Health and Social Care.

The CEO holds each line manager accountable for meeting objectives and to work together towards meeting the objectives approved by the Board.

6.3 Director of Nursing

The Director of Nursing is the Executive with delegated responsibility for implementation of Governance arrangements within the Trust.

The Director of Nursing and the Medical Director are responsible for overseeing the implementation of this document.

6.4 Medical Director/ Caldicott Guardian

The Medical Director is the appointed Caldicott Guardian for the Trust. The Caldicott Guardian is responsible for protecting the confidentiality of patient information and enabling appropriate information sharing.

6.5 Information Governance Manager/ Data Protection Office

The Trust Information Governance Manager (IGM) is the designated Information Governance management advisor for the Trust and has day-to-day responsibility for the management of all aspects of this service. They are responsible for advising all staff throughout the organisation on issues relating to IG which may affect them and the work they do.

The IGM is also the designated Data Protection Officer (DPO). This role is defined in Article 39 of the General Data Protection Regulation 2016 (GDPR), including providing leadership, challenge and support to achieve organisational compliance with the GDPR. The DPO will be required to fulfil the statutory functions and to report directly to the highest management level of the organisation.

The principal tasks of the DPO are to:

- Provide advice to the organisation and its employees on compliance obligations
- Advise on when data protection impact assessments are required and to monitor their performance
- Monitor compliance with the GDPR and organisational policies, including staff awareness and, provisions for training
- Co-operate with, and be the first point of contact for the Information Commissioner
- Be the first point of contact within the Trust for all data protection matters
- Be available to be contacted directly by data subjects

The IGM may delegate responsibility for investigation of incidents to the Information Governance & Privacy Officer, or other members of the IG team at their discretion.

6.6 Senior Information Risk Owner (SIRO)

The SIRO will act as an advocate for information risk for the Board of Directors.

The SIRO will ensure that identified information security threats are followed up and incidents are managed, and also ensure that the Board of Directors are kept up to date on all information risk issues.

6.7 All Staff

All staff across the Trust have a responsibility to ensure they comply with the policy and any associated strategies, policies, procedures and guidance.

Each member of staff shall be responsible for the operational security of the information systems they use and must comply with the security requirements that are currently in force. They will also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the Trust's information systems will be in operation. Staff drafting contracts will ensure that contractors and subcontractors of external organisations are required to comply with the Trust's Information Governance assurance framework with respect to policies, procedures, protocols guidelines and contractual obligations which are necessary to safeguard Trust information assets.

Advice can be sought by contacting the Caldicott Guardian, SIRO or Information Governance Manager in relation to all Information Governance queries.

Everyone working for the NHS has a legal duty to keep information about patients and clients and other individuals such as staff or volunteers confidential. They are required to adhere to confidentiality agreements i.e. common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

All staff are responsible for ensuring they keep up to date with Information Governance training in accordance with the Trust Statutory and Mandatory training policy (SWH 00564) as this training covers relevant data protection and confidentiality requirements.

7 Legislative Background

The Trust is obliged to abide by all relevant UK and EU legislation. The requirement to comply with this legislation will be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security for which they are responsible. The Trust will comply with the following legislation and other related legislation, guidance and codes of practice as appropriate:

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Access to Health Records 1990
- Human Rights Act 1998
- Computer Misuse Act 1990
- Health and Social Care Act 2015
- Caldicott Principles (from Caldicott Report 1997)
- 'To Share or Not To Share?' The Information Governance Review 2013
- The Confidentiality Code of Practice
- Information Security Management – ISO 17799
- Environmental Information Regulations 2004
- Records Management Code of Practice for Health & Social Care July 2016
- Data Security and Protection Toolkit
- Others may be included as Information Governance develops

8 Principles

8.1 Data Protection Act 2018 and GDPR

The Data Protection Act (2018) (DPA) and the General Data Protection Regulation (GDPR) sets out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

The DPA sets out 6 data protection principles which describe legal requirements in relation to data processing:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the 6 data protection principles is unlawful.

Although the Data Protection Act (2018) does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the Information Governance Team.

8.2 Information Commissioner's Office (ICO)

The ICO is the regulator for the DPA, GDPR and related legislation. Their role includes:

- Investigation of data breaches
- Investigation of concerns and complaints about an organisation's handling of data;

There are a number of powers the ICO have in relation to organisations. They could:

- Conduct an audit to ensure that legislation is complied with
- Serve an Enforcement Notice order, if there has been a breach, requiring an organisation to take specific steps to comply with the law
- Prosecute an organisation for failing to take appropriate action
- Issue a fine of up to £17 million, or 4% of annual turnover, whichever is higher.

The ICO can also prosecute and fine individuals for serious breaches of the Data Protection Act.

The Trust is required to register annually with the Information Commissioner as a Data Controller. The Trust's unique registration number is Z822711X.

8.3 NHS Caldicott Report

The Caldicott Report was published in 1997 (updated in 2013 and 2016) and focused on the protection and processing of patient identifiable information within the NHS. The reports provided the NHS with a series of principals to adhere to:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

The Trust appointed Caldicott Guardian is the Medical Director. They advise the Trust on matters of patient confidentiality and promote the safe and secure handling of patient data. The Trust Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures.

8.4 Data Security and Protection Toolkit (DSPT)

All organisations that have access to NHS patient data and systems must complete the DSPT to provide assurance that they are practising good data security and that personal information is handled correctly. It is an annual online self-assessment tool that requires organisations to measure their performance against the National Data Guardian's 10 data security standards:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

Each initiative is further divided into a number of 'Assertions' against which the Trust is required to assess and evidence its current compliance.

9 Procedures

9.1 Data Processing

Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between the Trust and its patients, staff and others with whom we deal.

The DPA requires that processing of any personal information held by the Trust must be both fair and lawful. This requires that the processing meets fair processing criteria and satisfies one or more 'conditions for processing' set out in the DPA.

To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold.

We must demonstrate that we:

- Are open and honest about our identity
- Tell people how we intend to use any personal data we collect about them
- Usually handle their personal data only in ways they would reasonably expect
- Do not use their information in ways that unjustifiably have a negative effect on them
- Help people to understand their rights

To meet this requirement the Trust publishes a Privacy Notice to inform patients about the way we handle and use their personal data. This is available on the Trust website.

Under GDPR there must be legal basis for processing personal information and an additional legal basis for processing special category data such as health information.

Most personal data within the Trust is processed under Article 6(e) of GDPR "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

Most special category is processed under Article 9 (h) of GDPR: "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional".

Where data is processed under a different legal basis, that basis must be made clear. The Trust's privacy notice has detailed information about the processing of patient's data and is available on the Trust website.

The legal bases for processing personal and special category data are shown at **Appendix A**. It should be noted that under GDPR, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". This should be used as the legal basis only when there is a clear basis for patients to consent and to withdraw their consent.

When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information. Refer to the Information Governance Accreditation and Privacy by Design Policy SWH 00319.

9.2 Information Security

The Trust will establish and maintain policies and procedures for the effective and secure management of its information assets and resources.

The Trust will promote effective confidentiality and security practices to its staff through policies, procedures and training.

The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Action plans will be developed following incidents to ensure that remedial action is taken to prevent similar breaches occurring again.

Information assets and information flows have been mapped and recorded and will be regularly reviewed to assess and prevent the unlawful and unnecessary use of personal identifiable information.

With regard to ensuring patient identifiable information is only used where appropriate, the Trust has implemented a pseudonymisation process in line with national guidance on secondary usage. Please refer to the Pseudonymisation Policy (SWH 00848) for more information.

9.2.1 Access to IT Systems

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access. The Information Security Policy (SWH 00530) provides detailed guidance on the security of Trust IT systems including minimum standards of access controls.

All staff are given access to systems containing information on a need to know basis and access levels to these is appropriately assigned.

Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access.

Existing system users should not allow others to access systems using their login credentials.

Staff must not share passwords, Smartcards, security passes or any other privilege access that they have been authorised to have.

Staff are responsible for all activity that takes place under their log-in, in whichever system. Any sharing of passwords, or other access may result in disciplinary action.

9.2.2 Removable media

Removable media includes: CDs, DVD, USB Memory Devices, Laptops, iPads, smartphones (this list is not exhaustive). All removable media must be encrypted using NHS approved encryption software. ICT Services can provide guidance on this.

For further details refer to the Information Security Policy (SWH 00530) and Mobile Device policy (SWH 01205). Request forms are available on the IG pages of the intranet.

9.2.3 Remote Working

The Trust allows staff to work remotely using encrypted laptops, encrypted USB sticks and via a secure VPN link or from home computing equipment (i.e. not Trust provided) using the secure Remote Desktop solution. Online access to Microsoft 365 services such as Teams and Outlook is also available from home computing equipment by using standard log on username and password.

The Trust permits staff with line manager and Caldicott Guardian approval to remove information off site providing it is justified and has been supported in writing and documented on a Working from home form available on the IG Intranet pages.

Staff wishing to access Trust email via an app on their personal device (mail app) can do so by signing the Bring Your Own Device (BYOD) form and requesting ICT to configure the email to be accessible on the device. If accessing emails or other Trust business on your personal device the Trust reserves the right to wipe your device remotely. This is because emails are stored on the device and have to be encrypted and protected.

9.2.4 Storage of Electronic Data

Electronic-based personal data should not be held on local hard drives (C: drives) but should be held in folders on shared network drives with access limited to authorised staff. Staff member's own personal information, e.g. their own appraisal documents, may be stored within 'My Documents'.

9.3 Access to Records

The Trust holds millions of individual patient records in a variety of formats. In addition, it holds personal records for present and former members of staff and others it does business with.

While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

Many of our digital clinical systems will allow a user to access any individual record held in that system. Users should only access individual personal records for those data subjects (patients, staff etc) that they have authorisation to access for specific purposes or in the case of patient records where they have a 'legitimate relationship' with the patient.

Staff have no right to access personal information held in records about their relatives or friends.

While some Trust staff are in a position to potentially access personal data held about them in Trust records (e.g. their personal medical records) this is not a facility available to members of the public. NHS policy is that NHS staff should follow the same procedure as members of the public to access their data. Therefore, Trust staff should not access their own data held in any Trust records without specific authorisation.

Procedures for obtaining access to or copies of personal information held by the Trust about individuals are explained in the Access to Health Records Policy (SWH 00422).

The Trust carries out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' record data may face disciplinary action. Further details are provided in the Unauthorised Access to Records Procedure SWH 04355.

9.4 Security of Personal Data

Personal data must not be left unattended, or where it might easily be accessed by a third party who is unauthorised to have this access.

This includes, for example:

- Leaving records on a desk in an unlocked and unmanned office
- Walking away from a pc without locking it
- Allowing another person access to your password inappropriately, or
- Positioning a pc screen such that it is readily visible to others e.g. in a reception area.

At the end of a working day, all confidential paperwork should be stored away in a drawer or filing cabinet, and not left on view, that is, following a 'clear desk' approach. If information cannot be stored away, you should ensure access is restricted e.g. by locking the office door or locking the department at the end of the day.

Paperwork which includes identifiable or confidential data must be securely shredded when no longer required or put into designated confidential waste sacks for commercial confidential disposal.

9.5 Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible information quality and accuracy should be assured at the point of collection.

The Trust will promote information quality and effective records management through policies, procedures and training. Please see the Trust's Information Data Quality Assurance Policy (SWH 00007) for more information.

9.6 Communicating Personal Information

In order to provide effective care services there is a need to transfer information between organisations and individuals. In order to comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any data containing identifiable information transferred by the Trust outside the Trust for processing must be securely encrypted during transit.

Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

A guide to staff on the transfer or communication of personal data by post, by hand and e-mail and the use of portable media is in **Appendix B**. Guidance on verbal communication is at **Appendix C**.

9.7 Disclosure and Sharing of Personal Information

9.7.1 Sharing Personal Information for Care Purposes

In order to provide safe and effective care, personal information about patients will need to be shared with all those caring for an individual. In addition to the clinical team providing care, the direct care team may include laboratory staff, social care staff, specialist care teams and administrative staff supporting the care process.

In accordance with both DPA2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate. In applying this principle care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

Caldicott principle 7 (Duty to share) emphasises the need to share information in certain circumstances where the duty to share information clearly outweighs the normal duty of confidentiality owed. This would be the case when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent that threat materialising.

9.7.2 Sharing Personal Information for Non-Care Purposes

Non-care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymised or pseudonymised data. This removes the need to consider consent issues. Further guidance on this topic can be found in the Pseudonymisation Policy SWH 00848.

In certain circumstances the law requires that confidential information should be disclosed when consent may not be provided. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease. Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

Non-confidential information may be made available to the public through a variety of means in line with the Trust's Freedom of Information Policy (SWH 00384).

Further guidance on specific aspects of information sharing and disclosure is given in **Appendices D & E**.

9.7.3 Access to Trust Data

If you are working with staff from other organisations who require access to Trust data they should complete the Data Access form. Access will be approved by the Caldicott Guardian

9.8 Disposal of Personal Information

It is a principle of the DPA that data should 'not be kept for longer than necessary'. The Trust follows The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 which is available on the intranet.

Any documents containing personal data should be disposed of securely and not discarded in domestic waste and recycling bins. The Trust waste management team operate a confidential waste disposal service and provide regular collections of confidential waste from all Trust areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through ICT to ensure all data is effectively removed before disposal.

Medical devices and equipment should be transferred, decommissioned and disposed of in line with the Medical Devices Policy SWH 00168.

10 Training

All staff are responsible for ensuring they keep up to date with annual Information Governance training in accordance with the Trust Statutory and Mandatory Training Policy (SWH 00564) as this training covers relevant data protection and confidentiality requirements.

11 Incident Reporting

Any breach of data protection and confidentiality can have severe implications for the Trust, our patients and staff and, where significant numbers of patients are involved, can impact on the reputation of the NHS as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 constitutes a serious disciplinary offence or gross misconduct under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

In the event of an incident relating to Information Governance it will be reported via the Incident Reporting system (Datix) as described in the Incident Management Policy including the Management of Serious Incidents (SWH 00020) and the Being Open and the Duty of Candour (SWH 00356).

12 Monitoring Compliance

The Information Governance Manager will ensure that the key processes set out in this document are audited in line with the DSP Toolkit requirements. The results will be fed back via the Information Governance & Security Steering Group.

Where monitoring has identified deficiencies, recommendations and an action plan will be developed to improve compliance with the document. See **Appendix F** for specific details.

13 Equality Impact Assessment

All Trust documents are required to have a preliminary Equality Impact assessment (EIA) performed on them in order to establish whether any group of people will be impacted on unfairly by the document. An EIA has been performed on this document and the outcome is shown in **Appendix G.**

14 Author

Information Governance and Privacy Officer

15 Contributors

Information Governance and Security Steering Group
Transmission procedure working group

16 References

University Hospital Southampton NHS Foundation Trust: Data Protection and Confidentiality Policy, 2018

South Warwickshire NHS Foundation Trust (2020) SWH 00007 Information Data Quality Assurance Policy

South Warwickshire NHS Foundation Trust (2019) SWH 00020 Incident Management Policy including the Management of Serious Incidents

South Warwickshire NHS Foundation Trust (2016) SWH 00168 Medical Devices Policy

South Warwickshire NHS Foundation Trust (2019) SWH 00169 Management of Healthcare Waste Policy

South Warwickshire NHS Foundation Trust (2018) SWH 00319 Information Governance Accreditation and Privacy by Design Policy

South Warwickshire NHS Foundation Trust (2019) SWH 00356 Being Open and the Duty of Candour

South Warwickshire NHS Foundation Trust (2020) SWH 00384 Freedom of Information Act Policy

South Warwickshire NHS Foundation Trust (2018) SWH 00422 Access to Health Records Policy

South Warwickshire NHS Foundation Trust (2014) SWH 00519 Email Usage Policy

South Warwickshire NHS Foundation Trust (2016) SWH 00530 Information Security Policy

South Warwickshire NHS Foundation Trust (2016) SWH 00848 Pseudonymisation Policy

South Warwickshire NHS Foundation Trust (2017) SWH 01626 Internet Usage Policy

South Warwickshire NHS Foundation Trust (2020) SWH 04355 Unauthorised Access to Data Procedure

South Warwickshire NHS Foundation Trust (2020) SWH 04359 Photography and Recording Policy

South Warwickshire NHS Foundation Trust (2020) SWH 04360 National Data Opt Out Policy

17 Appendices

Appendix A: Legal Bases for Processing Personal and Special Category Data

Appendix B: Guidance on the Secure Transfer and Communication of Personal Data

Appendix C: Guidance on Verbal Communication of Personal Data

Appendix D: Key Questions for Confidentiality Decisions

Appendix E: Disclosing Confidential Information

Appendix F: Monitoring Compliance Form

Appendix G: Equality Impact Assessment

18 Appendix A: Legal Bases for Processing Personal and Special Category Data

18.1 Lawfulness of processing personal data (Article 6 of GDPR)

Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given ***consent*** to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a ***contract*** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a ***legal obligation*** to which the controller is subject;

(d) processing is necessary in order to protect the ***vital interests*** of the data subject or of another natural person;

(e) processing is necessary for the ***performance of a task carried out in the public interest*** or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the ***legitimate interests*** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

18.2 Processing of special categories of personal data (Article 9 of GDPR)

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is lawful only if 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, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(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 law in so far as it is authorised by Union or Member

State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(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 is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a ***political, philosophical, religious or trade union aim*** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly ***made public by the data subject;***

(f) processing is necessary for the establishment, exercise or defence of ***legal claims*** or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of ***substantial public interest***, on the basis of Union or Member State 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;

(h) processing is necessary for the purposes of ***preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services*** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is 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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for ***archiving purposes*** in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State 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.

19 Appendix B: Guidance on the Secure Transfer and Communication of Personal Data

19.1 Introduction

Public sector organisations continue to report a high level of data beaches, many of which relate to the insecure transfer and inappropriate disclosure of sensitive personal information.

It is therefore important that all staff are aware of best practice and guidance for the secure transfer and communication of personal data.

Guidance for staff on the use of postal services, e-mail and fax to communicate and transfer personal data is outlined in this appendix. Guidance covering manual transfers and taking personal information off site is also provided.

Circumstances may arise where a transfer of personal data needs to take place but for some reason it is not possible to follow best practice and the proposed method of transfer poses a degree of risk. In these circumstances the sender must conduct a simple risk assessment and consider if the perceived need to communicate the data by the method selected outweighs the risk associated with the method of transfer.

For example, where there is an urgent need to communicate with another professional about a patient and no secure method of communication is available an insecure communication channel (including the minimum of personal identifiers) may be selected for use. Any such decisions should be documented.

19.2 Transporting paper documents

A high proportion of IG incidents relate to the loss of paperwork. Paper documents which include personal information may sometimes need to be transported across site, from one site to another, for home working, or when working in the community.

The loss of paperwork may present a clinical risk, in addition to a breach of confidentiality.

When transporting documents, you must:

- Consider whether you need to take paperwork out of a secure environment
- Consider whether information can be de-identified, e.g. by using initials instead of a patient's full name
- Transport it securely using:
    - A robust envelope
    - A tamper proof bag. These can be obtained from procurement.

You must not:

- Carry loose pieces of paper
- Use identifiable data if it is not needed

19.3 Post

All correspondence containing confidential or personal patient or staff identifiable information must always be addressed to a named recipient e.g. addressed to a named

person, a post holder, a consultant, a designated group not merely to a department or organisation.

Internal mail containing confidential or personal patient or staff identifiable information must only be sent in a securely sealed envelope and marked accordingly (e.g. “Confidential” or “Addressee Only”, as appropriate).

External mail containing confidential or personal patient or staff identifiable information must also be sent in a securely sealed envelope and marked accordingly e.g. “Confidential” or “Addressee Only”, as appropriate.

If deemed appropriate, sensitive/confidential mail, may be sent by special delivery. In some circumstances, it may also be advisable to obtain a receipt as proof of delivery.

- Check that all the information relates to the correct individual before sending out; and that information intended for another recipient is not included.
- Mark envelopes as ‘Private and Confidential’ when appropriate
- Use a robust, secure and sealed envelope
- Include a return address on the envelope
- Include your departmental budget code on the envelope
- Do not use window envelopes for bulk mailings

19.4 Email

Staff can securely email from their SWFT email account. This includes to other organisations, to NHS.net and to individuals.

The important thing is to consider what type of information you are sharing and with whom. As much as possible limit the use of personal/confidential patient information.

Emails which include bulk or highly sensitive information (e.g., safeguarding, sexual health, etc.) should be encrypted. If you do not have this facility, contact ICT to request the installation of the SOPHOS encryption facility on your machine. Please note, depending on priorities and resources, it may not be possible for a technician to install this immediately.

Always carry out the following basic checks:

- Are you using the correct email address?
- Are you sending the minimum/ appropriate information?
- Have you checked the email trail to ensure that only appropriate information is forwarded?

For more information, refer to the Trust’s Email Usage policy (SW 00519)

19.5 Instant Messaging

The Trust permits the use of Instant Messaging platforms which offer end-to-end encryption such as WhatsApp and Facebook Messenger. Patient or staff data is transmitted securely when using Instant Messaging. This includes the transmission of personal data such as name or date of birth, and special category or sensitive data including health details.

You must not:

- Allow anyone else to use your device
- Share excessive information
- Share clinical or corporate sensitive information outside of the relevant individuals or groups

You must:

- Use a messaging app which offers end-to-end encryption
- Minimise the amount of patient or staff identifiable data
- Include enough details for identification and decision making
- Set your device to require a passcode immediately, set it to lock out after a short period of not being used
- Disable message notifications on your device's lock-screen
- Enable the remote-wipe feature in case your device is lost or stolen
- Unlink the app from your photo library
- Communicate with the correct person or group, especially if similar names are stored
- Clearly separate your social groups from any work groups
- If you are an administrator of a messaging group, take great care when selecting the membership of the group, and review the membership regularly
- Update the medical record with details of advice given, etc.
- Delete the messaging notes once records have been updated
- Remember that instant messaging conversations may be subject to Freedom of Information requests or Subject Access Requests
- Communicate appropriately and consistently in line with the values and policies of the Trust

19.6 Fax

The Trust is currently in the transition of phasing out all outbound fax transfers to a secure email solution or other electronic system, in line with Department of Health and Social Care guidelines. For this reason no new fax transfers are to be introduced.

However during this transition any faxes containing personal or other sensitive information should be subject to processes to ensure faxes are safely stored, sent and received. Faxes must only be sent when there is no alternative.

20 Appendix C: Guidance on Verbal Communication of Personal Data

20.1 Introduction

Staff should remember the need to maintain security and confidentiality when discussing personal or other sensitive information, whether in face-face conversation, over the phone or via online meetings. This applies when discussing personal information of both staff and patients.

Confidential or personal information should only be provided to people who have a valid reason to know it. This applies to verbal information as well as written. By mishandling verbal information you may breach an individual's confidentiality.

20.2 Conversations

The security and confidentiality of telephone and personal conversations should be considered. Staff should be mindful of the need to maintain confidentiality and security when discussing personal or other sensitive information. Discussion around all clinical matters should be discussed in a secure environment instead of in corridors or in lifts; the same would apply around discussion around members of staff.

20.3 Phone Calls

20.3.1 Organisational

When communicating information over the phone to other organisations, staff should ensure they follow the Caldicott principles before they disclose any confidential or sensitive information, during this process staff should confirm:

- The name, job title, department and organisation of the person requesting the information
- Confirm the reason for the request
- Take a contact telephone number e.g. main switch board number, never a mobile number
- Check whether the information can be provided - tell the enquirer you will call them back
- Provide the information to only the person who requested it – do not leave messages on an answering phone or with another individual
- Ensure that you record your name, date, time of the disclosure, the reason for it and who authorise it, also record the recipient's name, job title, organisation and telephone number

Where the patient is conscious and competent their consent should be sought before information is disclosed. If this is not possible then decisions on whether to disclose should be made on a case by case basis taking into account the best interests of the patient and any legal authority in place. It is advised that decisions involving disclosures should always be documented.

20.3.2 Patient's Relatives & Friends

Information should generally only be disclosed to a next of kin, relatives or friends with the consent of the patient.

It is important to note that next of kin do not have any automatic right to patient information. Parents or those with parental responsibility have a right to information about their children unless the child has sought treatment independently of their parents. Personal information relating to outpatients should only be disclosed to the patient. For inpatients, all calls should be directed to the ward/ department where the patient is located.

Some wards and community services set up a password system whereby information is only provided when the password is disclosed.

20.3.3 Receiving Phone Calls from Patients

Staff should ensure they gain the best level of assurance of the patient's identity by obtaining confirmation of personal details, such as:

- Date of birth
- Address and post code
- Appointment dates
- Treatment/ clinic details
- Hospital or NHS number

20.3.4 Making Phone Calls to Patients

The patient's right to privacy means that when making outgoing calls we need to speak to the patient directly, unless it is justifiable to speak to someone else. i.e. the patient has provided their consent or it is in their vital interests.

Wherever possible if you think you may need to contact a patient by phone, obtain and document their preferences:

- Which number would they prefer to be called on?
- Would they like information left with a family member if they cannot be contacted directly?
- Are they happy for messages to be left on their answerphone?

20.3.5 Leaving Answerphone Messages

The use of answer phone messages with patients is not a preferred method of communication. There are privacy risks with leaving messages unless the patient has consented to this. There is a balance to be struck between respecting the privacy of the patient, not unduly worrying them with an obscure message and ensuring the recipient understands it is a genuine message.

Staff should consider whether any particular issues exist that could affect whether it is appropriate to leave an answer phone message. Consider the following:

- If you leave a message, the patient may not be the first to hear it
- Who else might hear the message?
- Are you sure you have dialled the correct number?
- Will the patient fully understand the content of the message

- How can you be certain the message has been received?
- You may inadvertently breach confidentiality because the patient's friends or relatives may not know the patient is receiving health care.

Messages on landline answerphones should only be left in an emergency.

20.3.6 SWFT Answer Machines

Messages left on Trust answer machines may contain personal or sensitive information such as:

- Names, addresses or phone numbers of patients
- Patient's health queries
- Health or social care professionals phoning with queries about patients
- Applicants for jobs advertised.

Therefore:

- Consideration should be given to which staff members have access to answering machines
- Password protected voicemail boxes should be used to control access where available

Where this is not available suitable physical protection must be in place e.g. locating the phone in a lockable office.

21 Appendix D: Key Questions for Confidentiality Decisions

A number of key questions have been distilled to ensure that the requirements of law, ethics and policy are adequately addressed when making decisions about the use or disclosure of confidential patient information. These key questions, outlined below, underpin the decision support tool provided at Annex C of the "Confidentiality: NHS Code of Practice"

Q1 If the purpose served by disclosing is not healthcare or another medical purpose, what is the basis in administrative law for disclosing?

A1 Public sector bodies should only do the things that they have been set up to do. Whilst medical purposes are permitted, disclosures to other agencies for other purposes may not be.

Q2 Is disclosure either a statutory requirement or required by order of a court?

A2 Although disclosure should be limited to that required and there may be scope to ask the court to amend an order, at the end of the day any disclosure that has either a statutory requirement or court order must be complied with.

Q3 Is the disclosure needed to support the provision of healthcare or to assure the quality of that care?

A3 Patients understand that some information about them must be shared in order to provide them with care and treatment, and clinical audit, conducted locally within organisations is also essential if the quality of care is to be sustained and improved. Efforts must be made to provide information, check understanding, reconcile concerns and honour objections. Where this is done there is no need to seek explicit patient consent each time information is shared

Q4 If not healthcare, is the disclosure to support a broader medical purpose?

A4 Preventative medicine, medical research, health service management, epidemiology etc are all medical purposes as defined in law. Whilst these uses of information may not be understood by the majority of patients, they are still important and legitimate pursuits for health service staff and organisations.

However, the explicit consent of patients must be sought for information about them to be disclosed for these purposes in an identifiable form unless disclosure is exceptionally justified in the public interest or has temporary support in law under section 251 (formerly section 60) of NHS Act 2006.

Patients can opt-out of information sharing for the purposes of research or planning. Refer to the National Data opt Out Policy SWH 004360 for further details.

Q5 Is the use of identifiable and confidential patient information justified by the purpose?

A5 Where the purpose served is not to provide healthcare to a patient and is not to satisfy a legal obligation, disclosure should be tested for appropriateness and necessity, with the aim of minimising the identifiable information disclosed and anonymising information wherever practicable.

Q6 Have appropriate steps been taken to inform patients about proposed disclosures?

A6 There is a specific legal obligation to inform patients in general terms, who sees information about them and for what purposes.

22 Appendix E: Disclosing Confidential Information

It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with the highest quality care. In particular, clinical governance and clinical audits might not be obvious to patients, and should be drawn to their attention. Similarly, the need to share information between members of different care teams and between different organisations involved in their healthcare provision should be explained. This is particularly important where disclosure extends to non-NHS bodies, such as Social Care Services.

Many uses of confidential patient information do not contribute to or support the healthcare that the patient receives. Very often these other uses are extremely important and provide benefits to society, such as medical research, public health, health service management and financial audit. However, as they are not directly linked to the healthcare that patients receive, it cannot be assumed that patients are happy for their information to be used in this way and so this must be checked.

Staff need to be aware that information disclosures of their personal information are also necessary at times to facilitate their employment and / or training. This may include, but is not limited to, disclosures to non-NHS bodies, such as training providers and support companies.

Disclosure of Patient Information
Staff must ensure that patients are made aware that the information the patient gives may be recorded and shared, and the purposes for which this may apply (e.g. direct provision of healthcare, clinical audit, research etc).

Staff should check that information about the choices available in respect of how information is used or shared is given, and whether the patient has any questions or concerns regarding this. Information for patients is available through a patient leaflet and the Privacy Notice, which are both available on the Trust's website. Staff should be able to answer any questions or concerns about the use of the personal information. If they are unable to answer the questions or concerns, staff should be able to direct the questions or concerns to their line manager or another member of staff who can provide the answer. If the line manager or other team member is unable to answer the questions or concerns, advice and guidance can be sought from the Caldicott Guardian, SIRO or information Governance Manager.

Patients may opt-out of sharing for research or planning purposes. Refer to SWH 04360 National Data Opt Out Policy for further details

Disclosing to other Organisations
There are some circumstances where a decision to disclose identifiable information for non-healthcare purposes without consent may be warranted. These include:

- In the public interest / to protect the public (e.g. murder, rape, serious risk of harm could warrant breaching confidentiality); and
- Court Order

In the public interest / to protect the public: Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and

punishment of serious crime and / or to prevent abuse or serious harm to others where they judge (on a case by case basis) that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the Trust's provision of a confidential service.

Definitions are not clear but examples include murder, rape, child protection concerns, assault or the spread of an infectious disease. However, all requests for information from the Police must be directed to the Information Governance department, as per section 5.6 'Requests for information by the police or media'.

Whoever authorises the disclosure must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning used and the prevailing circumstances. Disclosures should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies.

Where possible, the issue of disclosure should be discussed with the individual concerned and consent sought. Where consent is not given, the individual should be told of any decision to disclose against their wishes. This will not be possible in certain circumstances, for example where the likelihood of a violent response is significant, or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

Court Order
A written request from the Police that is backed by a Court Order, stating exactly what information is needed and its purpose. This does not require the consent of the patient but they should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with terms of the court order and to the bodies specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not germane to the case in question, they may raise ethical concerns with the judge or presiding officer. However, if the order is not amended it must be complied with. A clear and accurate record of the circumstances should be kept.

Legal Restrictions on Disclosure
There are special restrictions on disclosure in the following circumstances:

- Sexually transmitted diseases; and
- Human fertilisation and embryology

Sexually transmitted diseases
All necessary steps must be taken to ensure that any information capable of identifying an individual with respect to examination or treatment for any sexually transmitted disease (including HIV and AIDS) shall not be disclosed except:

- Where there is explicit patient consent to do so;
- For the purpose of such treatment or prevention; and
- For the purpose of communicating that information to only those staff directly involved with the treatment of persons suffering from such disease or the prevention of the spread thereof.

23 Appendix F: Monitoring Compliance Form

Title of Document	Information Governance Policy Incorporating Data Protection and Confidentiality	
Relevant Standards	**Health & Social Care Act**	**Other e.g. West Midlands Quality Review Service, Peer Reviews etc**
	Regulation 21	Data Security and Protection Toolkit

Monitoring/Audit Plan

Process / minimum requirement to be audited / monitored	**Lead**	**Tool/How**	**Written Reporting Frequency**	**Written Reporting Arrangements**
This policy and elements within will be subject to audits by the Trust's internal auditors	Internal Audit	DSP Toolkit	Ad Hoc	Internal Audit Reports presented to the Information Governance & Security Steering Group and the Audit Committee
Where there are advances / amendments in Trust practice or further guidance issued by DH then this Policy will be reviewed	Information Governance Manager	DSP Toolkit	October and March in line with the DSP Toolkit	Reported to the Information Governance & Security Steering Group
The above Table outlines the minimum requirements to be audited/monitored; additional audits will be commissioned in response to deficiencies identified within the service through morbidity and mortality reviews/benchmark data provided by CHKS or in response to national initiatives e.g. NICE, RCOG guidelines and CNST standards. **Lessons learnt and action plans will be shared with all the relevant stakeholders.**				

Name:	Vicky Dumigan	**Job Title:**	Information Governance Manager	**Date:**	27/07/2020

24 Appendix G: Equality Impact Assessment Form

Has an Equality Impact Assessment been carried out?	**YES**
Preliminary Stage 1 Equality Impact Assessment (must be completed if required*)	
What date was Stage 1 completed and published?	**March 2011**
Has a Full Assessment Stage 2 Equality Impact Assessment Tool been undertaken*?	**NO-NA**
If yes, what was the date of assessment and publication of Stage 2 and action plan?	**NO**