Walsall Healthcare NHS
NHS Trust

Document Title
Data Breach Policy and Procedure

Document Description	
Document Type	Policy
Service Application	Trust Wide
Version	1.2

Lead Author(s)	
	Compliance and Risk Manager
	Corporate Governance Manager

Executive Director / Director / Manager			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date below:			
Name	Director of Strategy and Improvement	Date	
Signature		01.04.2019	

Change History		
Version	Date	Comments
1	March 2018	New policy to ensure compliance with the General Data Protection Regulations
1.1	May 2018	Review following minor amendments
1.2	March 2019	Minor review to remove reference to the EU

Links with External Standards	
General Data Protection Regulations	
Caldicott Principles	
Common Law Duty of Confidentiality	

Key Dates	DATE
Ratification Date	Trust Management Board – 26 June 2018 Minute Number 03/18
Review Date	June 2021

Executive Summary Sheet		
Document Title:	Data Breach Policy and Procedure	
Please Tick (☑) as appropriate	This is a new document within the Trust	√
	This is a revised Document within the Trust	

What is the purpose of this document?

The purpose of this policy is to ensure that Walsall Healthcare NHS Trust is meeting its legal, statutory and regulatory requirements under the General Data Protection Regulation and to ensure that all personal and special category information is safe, secure and processed compliantly.

What key Issues does this document explore?

The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

Who is this document aimed at?

The policy relates to all staff (including permanent, fixed term, temporary, third-party representatives or sub-contractors, agency workers, volunteers and students.

What other policies, guidance and directives should this document be read in conjunction with?

International Transfers of Personal Data Policy
Safe Haven Policy
Records Retention Policy
Confidentiality Policy
Information Management and Technology Policy
Patient Records Policy
Privacy Notice Standard Operating Procedure
Incident Management Reporting Policy
Information Risk Policy
Information Sharing Policy

How and when will this document be reviewed?

The policy lead should review this policy every three years or sooner if there is a change in legislation.

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
	Compliance and Risk Manager
	Corporate Governance Manager

Circulated to the following for consultation

Name / Committee / Group
Information Governance Steering Group
Divisional Quality Teams
Members of Policies, Procedures Group
Uploaded onto the intranet for wider circulation

Version Control Summary

Significant or Substantive Changes from Previous Version
A new version number will be allocated for every review even if the review brought about no changes. This will ensure that the process of reviewing the document has been tracked. The comments on changes should summarise the main areas/reasons for change.

When a document is reviewed the changes should use the tracking tool in order to clearly show areas of change for the consultation process.

Version	Date	Comments on Changes	Author
1.0	March 2018	New policy to ensure compliance with the General Data Protection Regulations	Governance Manager
1.1	May 2018	Review following minor amendments	Corporate Governance Manager
1.2	March 2019	Minor review to remove reference to the EU	Corporate Governance Manager

Document Index		Pg No
1.	Introduction	5
2.	Scope	5
3.	Statement of Intent	5
4.	Roles and Responsibilities	7
5.	Procedure	10
6.	Audit and Monitoring	14
7.	Training	14
8.	Definitions	15
9.	Legal and Professional Issues	16
10.	Related Policies	16
11.	Impact Assessment	17

Appendices		Pg No
1.	Data Breach Incident Form	18
2.	Impact Assessment Procedure	20
3.	Checklist for review and approval of document	41
4.	Equality Analysis Form	44

1. Introduction

Walsall Healthcare NHS Trust are committed to our obligations under the regulatory system and in accordance with the General Data Protection Regulation (GDPR), and maintain a robust and structured program for compliance adherence and monitoring.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any data breaches, this policy states our intent and objectives for dealing with such a breach.

Although we understand that not all risks can be completed mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from the risks associated with processing data.

The protection and security of the data that we hold and use, including personal information, is paramount to us and we have developed data specific controls and protocols for any breaches involving personal information and data subject to the GDPR requirements.

2. Scope

The policy relates to all staff (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Walsall Healthcare NHS Trust) within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

3. Statement of Intent

The purpose of this policy is to provide Walsall Healthcare NHS Trust's intent, objectives and procedures regarding data breaches involving personal information.

As a regulated body, we have a dedicated compliance breach policy that covers breaches in regulations, legal requirements and our obligations. However, this policy is specific to personal information and the breach requirements set out in the GDPR.

As we have obligations under the GDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees if a personal information breach occurs. This policy also notes our processes for reporting, communicating and investigating any such breach.

Whilst it is Walsall Healthcare NHS Trust's aim to prevent data breaches where possible, we do recognise that human error and risk elements occur in business that prevent the total elimination of any breach occurrence. We also have a duty to develop protocols for data breaches to ensure that employees, supervising authority and associated bodies are aware of how we handle any such breach.

Walsall Healthcare NHS Trust's definition of a personal data breach for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that

leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our 'Privacy be Design' approach to protecting data, we also have a legal, regulatory and business obligation to ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred.

Our Information Security Policy & Procedures and GDPR Policy & Procedures provide the detailed measures and controls that we take to protect personal information and to ensure its continued security.

We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s).

We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including (but not limited to): -

- Pseudonymisation and encryption of personal data
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures testing on a regular basis to test, assess, review and evaluating the effectiveness of all measures and compliance with the general data protection regulations and codes of conduct
- Frequent and rolling training programs for all staff in the GDPR, its principles and applying those regulations to each role, duty and the company as a whole
- Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the general data protection regulations and the measures we have in place to protect personal information
- Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Data Protection Officer

Objectives

- To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information

- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect patient's and staff – including their data, information and identity
- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of the data breach *(where applicable)* with immediate effect and at the latest, within 72 hours after having become aware of the breach

4. Roles and responsibilities

Chief Executive
Ultimate responsibility for general data protection rests with the Chief Executive.

Medical Director (Caldicott Guardian)
Responsibility for ensuring that all patient related personal data is processed and managed in accordance with the Caldicott Principles. The Medical Director acts as the Trust's Caldicott Guardian with responsibility for patient confidentialty.

Director of Strategy and Improvement (Senior Information Risk Owner)
Responsibility for ensuring that all risks to information are identified and managed effectively in line with relevant legislation. The Director of Strategy and Improvement acts as the Trust's Senior Information Risk Owner (SIRO).

The Director of Strategy and Improvement has overall responsibility for the implementation, monitoring and compliance with the policy. This includes reporting to Trust executive groups or the Board as nescessary.

In addition, the Director of Strategy and Improvement has overall responsibility for:

- Information security
- Information governance
- Data quality related to patient information

Director of Organisational Development and Human Resources
Overall responisbility for ensuring data quality related to staff information and ensuring that the Trust standard contract includes clauses relating to staff responsibilities around information governance.

Corporate Governance Manager
Responsibility for ensuring there are information governance arrangements in place to allow for the processes laid out within this policy and procedure.

Data Protection Officer
Walsall Healthcare NHS Trust have appointed a Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with others to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

The Data Protection Officer has assumed the below duties in compliance with GDPR Article 39: -

- To inform and advise Walsall Healthcare NHS Trust and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions

- To monitor compliance with the GDPR, associated data protection provisions and Walsall Healthcare NHS Trusts own data protection policies, procedures and objectives

- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs

- To cooperate with the Supervisory Authority where required

- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter

- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the DPO will provide advice where requested with regards to any general data protection impact assessment and monitor its performance pursuant

- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing

- In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the indecent on the breach form and making any relevant and legal notifications. The Supervisory Authoirty will be notified by the Data Protection Officer via the Data Security and Protection Toolkit.

Designated Data Protection Officer
NAME: Sharon Thomas
POSITION: Corporate Governance Manager
ADDRESS: Walsall Healthcare NHS Trust, Town Wharf, Block 3, Cavell Close, Walsall
EMAIL:sharon.thomas@walsallhealthcare.nhs.uk or
data.protection@walsallhealthcare.nhs.uk
TEL: 01922 721172 ext 5806

Health Records Manager
Overall responisbility for ensuring the appropriate records retention and destruction standards are adhered to.

Information Asset Owners
Any member of staff who has assigned responsibility for an information asset within the Trust (i.e. any system (electronic or paper based) that holds Trust information) is designated an Information Asset Owner for the purposes of information governance.

Privacy Officers
It is the responsibility of the Trust's Privacy Officer's to investigate any breaches of confidentiality regarding information accessed via the Spine.

Information Governance Steering Group
The Information Governance Steering Group (IGSG) will have overall responsibility for:
The updating and amending of this, and all over information governance policies
Monitoring the action plans for the Information Governance Toolkit (IGT) and the information governance work plan
Ensuring the statutory regulations around information governance are adhered to

Data Quality Team
The Data Quality Team are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified.

Divisional Directors (DD; or equivalent)
Managers are considered to be equivalent to DD's for the purpose of responsibilities under policies if they are responsible for management of a significant service and report directly to an Executive or Associate Director.

Responsibilities include implementation, monitoring and compliance within the Division and ensuring staff witih the division adhere to the requirements of the policy.

Matrons, Senior Sisters (with day to day responsibility for ward management), Departmental Managers or equivalent
This group will be responsible for day to day implementation of the policy.

Also included will be responsibility for ensuring:

- All staff are aware of their role under the policy
- Staff complete their mandatory annual information governance training
- Records are kept as specified
- Incidents / issues are reported

All Staff
All staff must ensure they understand and adhere to the requirements of this policy.

5. Procedures

Walsall Healthcare NHS Trust has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur.

Due to the nature of our business, Walsall Healthcare NHS Trust process and stores personal information, special category personal informaiton and confidential data and as such, we have developed a structured and documented breach incident program to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

We carry out frequent risk assessments, reviews, audits and gap analysis reports on all processing activities and personal data storage, transfers and destruction to ensure that our compliance processes, functions and procedures are fit for purpose and are mitigating the risks wherever possible.

Breach Monitoring & Reporting
Walsall Healthcare NHS Trust has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment.

All data breaches are reported to this person with immediate effect, whereby the procedures and forms detailed in this policy are enacted.

All data breaches will be investigated, even in instances where notifications and reporting is not required and we retain a full record of all data breaches to ensure that gap and pattern analysis are used.

Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

Breach Incident Procedures

Identification of an Incident
As soon as a data breach has been identified, it is reported to the immediate line manager and the reporting officer (Data Protection Officer) immediately via Safeguard and telephone / emails so that breach procedures can be initiated and followed without delay.

Reporting incidents fully and with immediate effect is essential to the compliant functioning of Walsall Healthcare NHS Trust and is not about apportioning blame.

These procedures are for the protection of Walsall Healthcare NHS Trust, it's staff, patients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measure should be to stop any further risk/breach to the organisation, patient, third-party, system or data prior to investigation and reporting.

Breach Recording
Walsall Healthcare NHS Trust utilises initally Safeguard to report the incident and then subsequently the Breach Incident Form (Appendix A) for all incidents and is completed after every instance of a data breach, regardless of severity or outcome.

Completed forms are logged in the Breach Incident Folder (electronic or hard-copy) and reviewed against existing records to ascertain any patterns or reoccurrences.

In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the inident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form as well as utilising the root cause anlysis templates. The outcome of which is communicated to all staff involved in the breach in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (refer to section 6 of this policy). The Supervisory Authoirty will be notified by the Data Protection Officer via the Data Security and Protection Toolkit.

In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

Human Error
Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee is to be held.

A review of the procedure/s associated with the breach is to be conducted and a full risk assessment completed in accordance with Walsall Healthcare NHS Trust's existing Risk Assessment Procedures.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Formal action (in-line with the Trust's disciplinary procedures)

System Error

Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the Data Protection Officer to assess the risk and investigation the root cause of the breach.

A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause.

Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

Assessment of Risk and Investigation

The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.g. encryption)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

Breach Notifications

Walsall Healthcare NHS Trust understands that we have obligations and a duty to report data breaches in certain instances.

All staff are aware of these circumstances and we have strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without undue delay.

Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual. The Supervisory Authoirty will be notified by the Data Protection Officer via the Data Security and Protection Toolkit.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after us becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay.

Where a breach is assessed by the Data Protection Officer and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested.

Where Walsall Healthcare NHS Trust acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay.

In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without undue delay after becoming aware of a personal data breach.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Record Keeping
All records and notes taking during the identification, assessment and investigation of the data breach are recorded and signed by the Data Protection Officer and are retained for a period of 6 years from the date of the incident.

Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occuring.

6. Audit / monitoring arrangements

Monitoring Process	**Requirements**
Who	Data Protection Officer
Standards Monitored	• All data breaches are reported appropriately and relevant; breach investigation form and logs, are in use • All data breaches are investigated regardless of whether it is notified to the regulatory body and a record is retained
When	Annually
How	• Audits • Incident Reporting
Presented to	Divisional Quality Teams
Monitored by	Information Governance Steering Group
Completion/Exception reported to	Quality & Safety Committee

7. Training:

It is mandatory for **all staff** to complete their annual information governance training.

This training is **not optional** and failure to comply may result in disciplinary action.

Training can be accessed either via ESR or by attending a classroom based session or completing a workbook.

8. Definitions:

GDPR means the General Data Protection Regulation and for the purposes of this document, the acronym is also used to collectively describe all of the data protection laws that Walsall Healthcare NHS Trust complies with.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject means an individual who is the subject of personal data

Data controller means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor, means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Third Party means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Consent of the data subject means 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.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Cross Border Processing means processing of personal data which: -

- takes place in more than one Member State; or
- which substantially affects or is likely to affect data subjects in more than one Member State

Representative means a natural or legal person established, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Supervisory Authority means an independent public authority which is established by a Member State

Binding Corporate Rules means personal general data protection policies which are adhered to by Walsall Healthcare NHS Trust for transfers of personal data to a controller or processor in one or more third countries or to an international organisation

9. Legal and professional Issues

- GDPR
- Caldicott Principles
- Common Law Duty of Confidence
- Freedom of Information Act 2000
- Access to Information Act 2002

10. Related Polices:

International Transfers of Personal Data Policy
Safe Haven Policy
Records Retention Policy
Confidentiality Policy
Privacy and Personal Data Protection Policy
Information Management and Technology Policy
Patient Records Policy
Privacy Notice Standard Operating Procedures
Incident Management Reporting Policy
Information Risk Policy
Information Sharing Policy

11. IMPACT ASSESSMENT

11.1 Financial implications

The GDPR imposes substantial fines on data controllers and processors for non-compliance.

Fines are administered by the individual member states supervisory authorities; i.e. The Information Commissioner. These fines are categorised in two levels; lower level which may result in a fine of up to £7.9M, or 2% of the worldwide annual revenue of the prior financial year, whichever is greater or upper level which could be up to £17.5M, or 4% of the worldwide annual revenue, whichever is greater.

The upper level fine could be issued for infringements of the basic principles for processing, including conditions for consent, the data subjects' rights to access and the transfer of personal data to a recipient in a third country or an international organisation.

Appendix 1
Data Breach Incident Form

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
DDI:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO OF DATA SUBJECTS AFFECTED:		**NO OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			

BREACH NOTIFICATIONS:		
WAS THE SUPERVISORY AUTHORITY NOTIFIED?	**YES/NO**	
IF YES, WAS THIS WITHIN 72 HOURS?	**YES/NO/NA**	
If no to the above, provide reason(s) for delay		
IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?	**YES**	**NO**
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE/S REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: *(if applicable)*		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		

HAVE THE MITIGATING ACTIONS PRVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*

WERE APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE?	**YES/NO**
If yes to the above, describe measures	

Investigator Signature: _____ Date: _____

Investigator Name: _____ Authorised by: _____

Appendix 2

Introduction: Impact Assessments
The terms Privacy Impact Assessment (PIA) and General Data Protection Impact Assessment (GDPIA) are often used inter-changeably within the security and privacy worlds, but can sometimes have different meanings.

The PIA is a long-standing term for an assessment that looks at the effects and risks of privacy of a project or process, with privacy being considered and not just the data protection implications.

Whereas DPIA is the term the GDPR utilises for the risk-based approach and pre-assessments for high-risk processing.

For the purposes of this document, Walsall Healthcare NHS Trust expands upon the GDPR requirements as set out in the Regulation and encompasses privacy as a whole, with all aspects and facets being included and considered.

We use the DPIA reference, but aim to exceed the Regulation requirements, using The Article 29 Working Party *'Guidelines on Data Protection Impact Assessment (GDPIA)*', as well as the ICO reference to "*Privacy Impact Assessments"* (PIA).

General Data Protection Impact Assessments (DPIA)
General Data Protection Impact Assessments (GDPIA) are a requirement of the GDPR and a tool that can assist those with data protection obligations in identifying the risks associated with data processing and posed to data subjects.

It enables a pre-emptive approach to assess the risks and apply corrective actions and mitigating controls before a breach occurs.

This DPIA document accompanies our GDPR Policy & Procedures and aids in the privacy by design ethos advocated in the General Data Protection Regulation (GDPR) 2016/679).

Article 35 of the Regulation provides the situations and provisions for DPIAs and require those obligated under the GDPR to have processes in place to assess data protection risks and identify when a DPIA is required.

The overall aim of the Walsall Healthcare NHS Trust's DPIA is to apply solutions and mitigating actions where a processing activity is deemed likely to cause a high risk to one or more individuals. The mitigating actions are then implemented into the project plan and then reassessed to ensure that the risk(s) has been eliminated or reduced to an acceptable level*.*

The overall scope of the risk solutions is to either: -

- Terminate
- Treat
- Transfer
- Tolerate

Where an impact assessment report indicates that the processing involved will or is likely to, result in a high risk to an individual(s) and we are unable to mitigate such risk(s) with appropriate measures or controls, the Data Protection Officer must consult the Supervisory Authority prior to the processing taking place.

When is an assessment necessary?
Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by any organisation.

When the risks of processing are high, we employ the use of DPIAs to assess the risk, the impact and the likelihood and document the origin, nature, particularity and severity of that risk, along with the processing purpose, reasons and mitigating measures and/or proposed solutions.

We rely on the Article 35(3) conditions and accompanying recitals as to when completing an impact assessment is necessary.

This list is included below; however, it is not exhaustive and we assess each processing activity on its own merits and carry out a DPIA where we believe that the processing is likely to result in high risk.

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)

- Processing on a large scale of special categories of data

- Processing on a large scale of personal data relating to criminal convictions and offences

- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)

- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual

- Those involving the use of new technologies

- New processing activities not previously used

- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects

- Processing activities making it difficult for the data subject(s) to exercise their rights

How do you undertake an assessment?
A lead is appointed within the department/area who is undertaking the processing activities. They will carry out the GDPIA, follow the process, record the necessary information and report the results to the Senior Management Team.

All GDPIAs are carried out in conjunction with the Data Protection Officer who provides advice and support for the compliance of the processes with the GDPR rules.

Where there are systems and/or new technologies involved, an I.T representative should be involved in the assessment.

If the screening questions indicate that an impact assessment is required, the Lead will assess the processing operations that will be involved in the DPIA (using the positively answered screening questions) and decide if any further team members are required.

This includes choosing specific team members who: -

- Understand the project's aims and the organisation's objective
- Authority to influence the design and development of the project and participate in decisions
- Expertise in data protection and compliance matters
- Ability to assess and suggest solutions to risks and develop mitigating actions
- Ability to communicate effectively with stakeholders and management
- The Lead can at any point in the process, engage other members to assist in specific areas as they deem fit or necessary.

GDPIA Stages
We have divided the Privacy Impact Assessment into stages to ensure that all aspects are covered, reviewed and documented.

Each stage is covered in detail under its category heading.

We have also provided the complete impact assessment templates in an Excel format so that you can assess each DPIA project in an electronic or hard copy format. Please contact the Data Protection Officer to request the electronic version:

Designated Data Protection Officer
NAME: Sharon Thomas
POSITION: Corporate Governance Manager
ADDRESS: Walsall Healthcare NHS Trust, Town Wharf, Block 3, Cavell Close, Walsall
EMAIL:sharon.thomas@walsallhealthcare.nhs.uk or
data.protection@walsallhealthcare.nhs.uk
TEL: 01922 721172 ext 5806

- **Stage 1.** *Identify the Need for a General Data Protection Impact Assessment* - review the GDPR Article 35(3) conditions in conjunction with the Data Protection Officer and use the screening questions to ascertain if the processing is likely to result in high risk to individuals

- **Stage 2.** *Project Brief & Plan* - description of the information flows, what data is being processed, where it is coming from, who it is going to etc

- **Stage 3**. *Identify the Risks* - risks will include those to individuals, the organisation and compliance (law/regulation breaches) and after speaking to management, employees and stakeholders

- **Stage 4**. *Identify and Evaluate Privacy Solutions* - develop and document corrective actions, solutions and mitigating controls that can reduce or eliminate the risks. Evaluate costs and benefits of each solution

- **Stage 5**. *Integrate Outcomes* - the solutions and actions to reduce/remove the risks must be added back into the project plan so that the risks can be reassessed with the mitigating actions in place

- **Stage 6.** *Authorisation & Recording* - all stages of the DPIA must be recorded using the provided templates and sign off must be obtained from the DPIA Lead, DPO and Director/Senior Manager

Identify the Need for an Impact Assessment
Not all processing activities will require a GDPIA to be completed, it is therefore essential that we carry out a check and use our predefined screening questions to ascertain which (if any) of the high-risk operations we intend to carry out, will require an impact assessment to be completed.
The questions provided in the screening template cover most of the risks that could be classed as high to a data subject and can be used prior to each assessment proposal, however we also judge each processing operation on its own merits and add questions if they are specific to the project or objective.

We also start our internal and external consultations at this stage and involve stakeholders, employees, senior management and any associated third parties who play a part in the processing or can lend insight and feedback to the processing operation and proposed risks. If any risks are identified via consultations, these are also added to our impact assessment template.

Note: Each screening question should be answered and you should add any new relevant question at the bottom dependant on the risk and/or processing operation you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and the areas to focus on.

REF	SCREENING QUESTION	YES	NO	N/A	NOTES
1	Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects of an individual(s)?				
2	Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)				
3	Is the processing on a large scale and involves special categories of data?				
4	Is the processing on a large scale and involves data relating to criminal convictions				

	and offences?				
5	Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (*i.e. CCTV*)				
6	Will the project involve the collection of new information about individuals?				
7	Will the project compel individuals to provide information about themselves?				
8	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?				
9	Is the information about individuals likely to raise high risk privacy concerns or expectations?				
10	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?				
11	Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?				
12	Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?				
13	Will the project require you to contact individuals in ways which they may find intrusive?				
14	Will any of the processing activities make it difficult for the data subject(s) to exercise their rights?				
15	Will the operation involve processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects?				
16	Will the processing involve individuals who are considered 'vulnerable'?				
17	Does the processing operation involve any significant risk of the personal information being leaked or accessed externally?				

If you answered **NO** to <u>all</u> the screening questions, it is unlikely that you will need to carry out a DPIA. You should retain a copy of this completed sheet along with your justification for any your answers in the notes section.
If you answered **YES** to one or more of the screening questions, you should proceed through the DPIA stages and complete the full impact assessment. When completed, a copy of your finished screening questions, answers and notes should be retained along with the recorded PIA documents.

Project Brief & Plan
Where data is obtained and how it is processed, stored and destroyed, is an essential part of a privacy impact assessment and as such, we utilise our existing Information Audit (*Information Asset Register*) data to complete this part of the assessment.

It is best practice and a GDPR recommendation that all organisations complete an Information Audit to record, categorise and protect the personal data that you hold and process.

The information audit enables us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller/processor and includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Access level (*i.e. full, partial, restricted etc*)

We use the data on the existing Information Audit to help us populate the below project brief and plan. This plan serves as the basis for carrying out the audit and for demonstrating our compliance with the GDPR impact assessment requirements. We understand that an incomplete understanding of how information is obtained, processed and stored, can be a risk itself and must be documented to ensure a full assessment is possible.

Examples:

(a) If we do not know how data has been obtained, we are unlikely to be able to verify the consent.
(b) If we have not documented and evidenced that we have met all the lawfulness of processing conditions when the data was obtained, we may be unfairly processing information or be preventing an individual from exercising their data protection rights.

How information audits are documented is bespoke to each business and can involve several methods to ensure a complete profile of the data is obtained and accessible. We use one or more of the below methods for recording the personal information obtained, processed, stored and transferred by us: -

- Information Audit
- Data maps
- Information flow charts
- Information asset register

The project brief and plan template also consists of the project background information, such as objectives, purpose, proposals, consultation reviews, outline/summary and previous DPIAs.

This gives an overall picture of the project and enables a better assessment of the privacy impact and risks.

The third part of the project brief and plan template is the main assessment questions which provide the basis for identifying the risks. The questions are predefined; however, we do add to these if the project requires specific questions or assessment criteria.

A DPIA is intended to be flexible and can accommodate any form of processing assessment.

The responses to the assessment questions then give us the issues and associated risks that are transferred over to the Privacy Issues and Risks template, detailing who is impacted, how they are impacted and providing a risk rating.

DPIA PROJECT BRIEF & PLAN			
PROJECT NAME:			***DIRECTIONS:*** *1. Complete each section and answer all the assessment questions.* *2. Use the reference number to refer to any responses that pose a risk and complete the Privacy Issues & Risks template.* *3. Provide as much detail as possible to ensure a complete assessment is made.*
PIA LEAD:			
DATE:			
CONTACT DETAILS:			
1. PROJECT BACKGROUND			
1.1	**PROJECT SUMMARY:** *Give an outline of the project, the processing and describe what is being planned.*		
1.2	**OBJECTIVES:** - *What are the aims of this project? What do you want to achieve from the processing? Why is it important/beneficial?*		
1.3	**PURPOSE:** - *What is the purpose of obtaining and processing the data?*		
1.4	**POTENTIAL RISKS:** - *Prior to carrying out the assessment question section, are there any privacy impacts or risks that have already been identified?*		
1.5	**CONSULTATIONS:** - *What insights or feedback have been obtained through consultations with stakeholders, third-parties and employees?*		
1.6	**EXISTING DATA:** - *Have any previous PIAs or compliance assessments been carried out on similar processing activities that can provide*		

	guidance for this assessment?	
1.7	**SYSTEMS/TECHNOLOGY:** - *If the processing involves the use of new technology or systems, provide any relevant information obtained from the initial implementation assessment of such systems.*	
1.8	**OTHER:** - Detail any other *information or suggestions that can add to the impact assessment?*	

2. INFORMATION AUDIT			
PERSONAL DATA		**JUSTIFICATION**	**PROCESSING ACTIVITY**
What data will be collected?		*Why does this data need to be collected? Is there anything you can omit if not necessary?*	*What processing operation(s) will the data be used for?*
Name			
Address			
Postcode			
DOB			
Age			
Gender			
Email Address			
Home Tel No.			
Mobile Tel No.			
NI Number			
NHS Number			
Income/Expenses			
Employment Data			
Ethnic Origin			
Religion			
Health Details			
Convictions			

Credit Data			
Other			

3. ASSESSMENT QUESTIONS		
REF	**ASSESSMENT QUESTIONS**	**RESPONSE**
3.1	*What is the legal basis for processing the information?*	
3.2	*Who will have access to the information?*	
3.3	*Will there be restrictions applied to access?*	
3.4	*Does the data need to be transferred to a third-party?*	
3.5	*Do you have safeguards in place for transferring?*	
3.6	*Will you need to obtain consent to process?*	
3.7	*How will consent be obtained and the right to withdraw consent be made available?*	
3.8	*Will you have control over the data and be able to update/complete it where applicable?*	
3.9	*Will you be using data minimisation techniques?*	
3.10	*Will data be encrypted and/or pseudonymised?*	
3.11	*How will information be destroyed after it is no longer necessary?*	
3.12	*How will information be stored?*	
3.13	*Will you be able to act on all rights of data subjects? (i.e. objections, rectifications, erasure, access etc)*	
3.14	*Will you be able to meet the deadline for supplying information?*	
3.15	*Does the processing operation require the Supervisory Authority to be notified?*	
3.16	*What security measures are in place to protect identifiable information?*	
3.17	*Have all employee, agents and third-parties involved in the project been trained on the data protection regulations and impact risks?*	
3.18	*What consultations are involved in identifying the privacy issues and risks associated with this project?*	

3.19	*Detail any other factors or information that can assist in this Privacy Impact Assessment.*	

Identify the Risks and Privacy Issues
Using the responses obtained from answering the assessment questions, we are now able to identify the privacy issues and associated risks and record who these risks will impact.

Risks will usually fall into one of three categories: -

- ***Risks to Individuals*** - Any risk that affects a data subject, their data, their privacy or their rights is classed as a risk to an individual. Inadequate disclosure controls, consent issues, processing purposes and surveillance methods are just a few of the issues that may result in risks to individuals.
- ***Compliance Risks*** - These can arise where the assessment response indicates that a breach of laws, legislation and/or regulations will occur if the processing goes ahead. This can include non-compliance with the GDPR, PECR or human rights legislation.
- ***Corporate Risks*** - Risks that will affect the business, including reputation, revenue, fines and sanctions. These will mainly arise where the initial collection, consent, disclosures, sharing and storage of the personal information have not been complied with or where record keeping is ineffective.

Once the risks have been identified, the below risk matrix is used to give the risk a rating based on the severity of the impact and the likelihood of the risk occurring. This rating provides an easy to see colour code for how severe the risk could be to the privacy of individual and therefore the necessity of putting mitigating actions into place.

The risk rating table below is based on the Trust's risk management strategy scoring matrix and the scores are based on the consequence versus the likelihood (risk scoring = consequence x likelihood (C x L)).

	Likelihood Score (L)				
Consequence Score (C)	**1**	**2**	**3**	**4**	**5**
	Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Catastrophic (5)	5	10	15	20	25
Major (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Minor (2)	2	4	6	8	10
Negligible (1)	1	2	3	4	5

For grading risks, the scores obtained from the risk matrix are assigned grades as follows:

	1 – 3	Low risk
	4 – 6	Moderate risk
	8 – 12	High risk
	15 – 25	Extreme risk

The following table should be used to decide upon the most appropriate likelihood for a particular threat:

Likelihood	Description	Summary
1	Rare	Has never happened before and there is no reason to think that it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Possible	On balance, the risk is more likely to happen than not
4	Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost certain	Either already happens regularly or there is some reason to believe it is virtually imminent

The following table should be used to decide upon the most appropriate consequence for a particular threat:

Consequence	Description	Effect on Patients/Staff	Financial Cost	Health and Safety	Damage to Reputation	Legal, Contractual, Trust Compliance
1	Negligible	No effect	Very little or none	Very small additional risk	Negligible	No implications
2	Minor	Some local disturbance to normal business operations	Some	Within acceptable limits	Slight	Small risk of not meeting compliance
3	Moderate	Can still deliver service with some difficulty	Unwelcome but can be borne	Elevated risk requiring immediate action	Moderate	In definite danger of operating illegally
4	Major	Business is crippled in key areas	Severe effect on income	Significant danger to life	High	Operating illegally in some areas
5	Catastrophic	Out of business, unable to provide a service	Crippling	Real of strong potential loss of life	Very high	Severe fines and possible imprisonment of staff

GREEN - Where an assessment outcome is Green, we still work to see if we can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible.
However, most green rated risks are acceptable and so focus should be placed on those with higher ratings.

Even where a green rating has been given at the risk/privacy identification stage, this risk is still to be added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.

YELLOW - Where an assessment outcome is Yellow, we work to see if we can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible.

AMBER - Where an assessment outcome is Amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (*acceptable)* level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and have to be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.

RED - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level.

Some processing activities are eliminated at this point as the impact to individuals is considered too high risk to proceed.

However, in instances where the activity is essential or is a legal requirement, the proposed solutions and mitigating actions are applied and a further DPIA to see if the subsequent DPIA results in a Green and/or acceptable level of risk.

If a high risk still exists and the processing activity is authorised, we always consult the Supervisory Authority (SA) prior to processing and advise that the DPIA indicates that the processing would result in a high risk and there is an absence of measures that can be taken to mitigate the risk. We then await written advice from the SA and provide all information requested by them during this period.

The above process enables us to devise ways to reduce or eliminate privacy risks and assess the costs and benefits of each approach, as well as looking at the impact on an individual's privacy and the effect on the processing activity outcomes.

This enables us to document our identification and assessment of the risk, the solutions and mitigating actions used to reduce or eliminate the risk and records privacy risks which have been accepted as necessary for the project to continue.

IDENTIFIED PRIVACY ISSUES AND ASSOCIATED RISKS					
REF	**PRIVACY ISSUE**	**RAG**	**RISKS TO INDIVIDUAL(S)**	**COMPLIANCE RISK**	**CORPORATE RISK**
#	*Use assessment response to detail the privacy factor resulting in risk*	*Risk Rating*	*Complete if risk impacts data subject(s) or put N/A if not applicable*	*Complete if risk causes non-compliance or put N/A if not applicable*	*Complete if risk impacts business or put N/A if not applicable*
PR1	*E.g. Processing relies solely on using automated systems*	*15*	*Affects rights under Article 22(1)* *Could result in biased results*	*Breaches Article 22(1)*	*Sanctions & fines for breaching GDPR*
PR2	*E.g. Processing makes it difficult to withdraw consent once given*	*6*	*Affects right to withdraw consent* *Unlawful processing*	*Breaches Article 7(3)* *Unlawful processing*	*Breach fines* *Reputational damage*

Identify and Evaluate Privacy Solutions
Once all privacy issues and risks have been identified and rated, we begin identifying and evaluating solutions and mitigating actions.

We address each issue and document measure and controls that will reduce the risk impact. It is not possible to terminate all risks, but we aim to reduce them to an tolerable level. Where unable to reduce risks to this level, we decide on cancelling the project or, accepting the risk if there is a legal/best interests' requirement.

Our aim is always to assess whether the impact on privacy is proportionate to the objectives of the project and to ensure that individuals and their privacy remains our priority. We consider any solution that may reduce risk and balance the aims with the impact.

When applying the solutions to the template, we use the risk rating obtained in the Risk Identification process to ensure that we know the current risk and what an acceptable level would be.

Once all solutions have been added, we are then able to repeat the assessment of the risk and ascertain its eliminated, reduced or accepted result.

The new risk rating is then added to the template.

Some of the steps we may use or consider reducing risks include: -

- Changing the personal information collected to reduce the privacy level when processing
- Carry out all processing in-house to avoid transfers or data sharing
- Utilise systems/technology to make the processing more accessible
- Creating new procedures for areas such as retention, destruction methods, exercising rights
- Developing new security measures for a specific project that align with its aims
- Ensuring that adequate and effective training is provided to staff of the general data protection regulations and the project processing
- Publishing guidance manuals and supporting documents for use by those involved in the project
- Creating new materials and website content to enable us to better communicate with individuals
- Carrying out higher level of due diligence on any processors used for the project
- Producing data sharing agreements and transfer contracts
- Having all involved in the project sign non-disclosure and confidentiality agreements

We also assess the costs and benefits associated with all solutions to ensure that they are viable, feasible and proportionate to the privacy impact.

All solutions also involve a review and input from the Data Protection Officer, who reviews them against the GDPR and any codes of conduct that we follow in accordance with general data protection laws.

PROPOSED RISK SOLUTIONS AND MITIGATING ACTIONS						
REF	**RISK**	**RAG**	**SOLUTION/MITIGATING ACTIONS**	**RESULT**	**OUTCOME**	**RAG**
#	*Risk to be mitigated*	*Current rating*	*Detail corrective actions, solutions and mitigating controls that address the risk*	*Treated, Tolerated, Terminated, Transferred*	*Has the solution(s) reduced the risk enough to proceed with processing?*	*New risk rating*
PR1	*E.g. Processing relies solely on using automated systems*	*15*	*1. After processing completes, add human intervention stage to assess results for bias.* *2. Add system trigger to wait for human sign off*	*Risk Terminated*	*Processing no longer relies solely on automated system as human intervention added, so risk is eliminated*	*1*
PR2	*E.g. Difficult to withdraw consent once given*	*6*	*Create communication to be sent to individual(s) with guidance for withdrawing consent in writing.*	*Risk Treated*	*Due to type/location of processing, withdrawal of consent can only be done in writing. Can't offer opt-out or automated withdrawal options at this time*	*6*

Integrate Outcomes
Once all risks and privacy issues have been identified and mitigating actions and solutions applied to tolerate, treat, terminate or transfer the risks, making the project viable, we then integrate the outcomes back into the project and create an action plan for developing and implementing the solutions.

The integrated outcomes template enables us to record what actions must now be taken to put the solutions identified above, into place. We also detail who has overall responsibility for ensuring that the actions are on track and completed, an estimated completion date and the status of the progress, so that any delays can be recorded and other parties can see how far along we are in the process.

The action plan also allows us to ensure that all risks and solutions have been accounted for and are being mitigated against and that no actions are missed or stall.

If at any point in the project, the objectives or processing operations change or need to be amended, we repeat the screening questions to ascertain if any new risks or privacy issues have been identified and then add these to the DPIA and provide solutions and action plan for them also.

The screening questions and assessment questions are revisited after all actions are complete to ensure that they are still appropriate and that solutions have reduced or eliminated the risks.

INTEGRATING OUTCOMES INTO PROJECT PLAN				
REF	**ACTION(S) TO BE TAKEN**	**RESPONSIBILITY**	**COMPLETION DATE**	**PROGRESS/STATUS**
#	*Details what actions must happen for the solutions in the evaluation plan to be developed and implemented*	*Who is responsible for overseeing the actions and updating the project plan*	*What is the expected date that the actions will be completed*	*Current progress and/or action status*

Authorisation & Recording
All stages and aspects of a DPIA are recorded and retained for 6 years after the project implementation date. These are also used again should a similar project or technology be utilised in the future.

The stages in the DPIA aim to demonstrate that we are carrying out effective assessments when high risks to privacy are involved and that the security and privacy of personal data is one of our main priorities.

Keeping records of all stages enables us to evidence that we have identified, assessed and mitigated at every stage and that all risks have been evaluated.

Where there is a requirement for us to send a copy of the DPIA report to the Supervisory Authority, we do this within the deadlines and await their authorisation to proceed before going ahead with any processing.

Such disclosures include the full report, along with a summary of the project, risks and proposed solutions.

The finalised DPIA is authorised by the Data Protection Officer, DPIA Lead and a member of the Director/Senior Management team.

Appendix 3

Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any procedural document that requires ratification

	Title of document being reviewed:	Yes/No	Comments
1.	**Title**		
	Is the title clear and unambiguous? It should not start with the word policy.	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated? This should be in the purpose section.	Yes	
3.	**Development Process**		
	Does the policy adhere to the Trust policy format?	Yes	
	Is the method described in brief? This should be in the introduction or purpose.	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
	Are all terms clearly explained/defined?	Yes	
5.	**Evidence Base**		
	Has a comprehensive literature search been conducted to identify best evidence to inform the policy?	Yes	
	Have the literature search results been evaluated and key documents identified?	Yes	
	Have the key documents been critically appraised?	Yes	
	Are key documents cited within the policy?	Yes	

	Title of document being reviewed:	Yes/No	Comments
	Are cited documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	No	
	For Trust wide policies has the appropriate Executive lead approved the policy?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**	Yes	
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?	Yes	

Reviewer			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name		Date	
Signature		Approving	IGSG/Policies and Procedures Group and Trust Executive Committee

		Committee/s	

Lead Manager (Local Policies) / Director (Trust Wide Policies)			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name	Sharon Thomas	Date	May 2018
Signature		Approving Committee/s	IGSG/Policies and Procedures Group and Trust Executive Committee
Ratification Committee Approval			
Quality Board minute number: PPG minute number: **TMB minute number:**			

Service Overview & Improvement Action Plan: Equality Analysis Form

Title: **Data Breach Policy and Procedure**	What are the intended outcomes of this work? **The purpose of this policy is to ensure that Walsall Healthcare NHS Trust is meeting its legal, statutory and regulatory requirements under the General Data Protection Regulation and to ensure that all personal and special category information is safe, secure and processed compliantly.**
Who will be affected? **All Staff**	Evidence: **N/A**

ANALYSIS SUMMARY: considering the above evidence, please summarise the impact of the work based on the Public Sector equality duty outcomes against the 9 Protected characteristics			
Public Sector Duty *Protected Characteristics* (highlight as appropriate)	**Eliminate discrimination, harassment and victimisation**	**Advance equality of opportunity**	**Promote good relations between groups**
AGE / DISABILITY/ RACE	*This may refer to vulnerable adults and vulnerable safeguarding children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*

SEX (Gender)/ GENDER REASSIGNMENT	*Refer to Gender Recognition Act 2004*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
RELIGION or BELIEF/ SEXUAL ORIENTATION	*This may refer to vulnerable adults and vulnerable safeguard children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
PREGNANCY & MATERNITY	*This may refer to vulnerable adults and vulnerable safeguarding children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
MARRIAGE & CIVIL PARTNERSHIP	*No impact*	*Not applicable at present*	*Not applicable at present*

What is the overall impact? There are no negative implications associated with this policy. The implementation promotes positive opportunities and relationships between all groups and is in accordance with the new General Data Protection Regulations.			
Any action required on the impact on equalities? Impact of this policy has been assessed and it will not lead to any discrimination or other adverse events on any population groups, as described above.			
Name of person completing analysis	*Corporate Governance Manager*	**Date completed**	*May 2018*
Name of responsible Director	*Director of Strategy and Improvement*		
Signature			