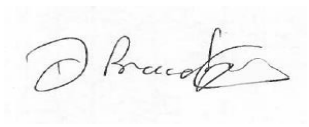
Walsall Healthcare NHS
NHS Trust

Document Title
General Data Protection Regulations (GDPR) Policy and Procedure

Document Description	
Document Type	Policy
Service Application	Trust Wide
Version	1.1

Lead Author(s)	
Kirstie Macmillan	Compliance and Risk Manager
Sharon Thomas	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	Daren Fradgley	Date	May 2018
Signature			

Change History		
Version	Date	Comments
1.0	March 2018	New policy to ensure compliance with the General Data Protection Regulations
1.1	May 2018	Combine Standard Operating Procedures and Audit Tool prior to approval

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	May 2020

Executive Summary Sheet		
Document Title:	General Data Protection Regulations (GDPR) 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
Data Breach Policy
Information Management and Technology Policy
Privacy Notice Standard Operating Procedure
Patient Records Policy
Information Risk Policy
Information Sharing Policy
Privacy and Personal Data Policy
Incident Management Reporting Policy

How and when will this document be reviewed?

The policy lead should review this policy in 2 years or sooner if there is a change in legislation.

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
Kirstie Macmillan	Compliance and Risk Manager
Sharon Thomas	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	Kirstie Macmillan
1.1	May 2018	Combine Standard Operating Procedures and Audit Tool prior to approval	Sharon Thomas

1. Introduction

Walsall Healthcare NHS Trust needs to collect personal information to effectively and compliantly carry out our everyday business functions and activities.

Such data is collected from employees, patients and service users and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection laws and specific data protection codes of conduct (herein collectively referred to as 'the GDPR').

Walsall Healthcare NHS Trust has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the GDPR and its principles, including staff training, procedure documents, audit measures and assessments.

Ensuring and maintaining the security and safety of personal and/or special category data belonging to the individuals with whom we deal is paramount to our ethos and Walsall Healthcare NHS Trust adheres to the GDPR and its associated principles in every process and function.

GDPR was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to the Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As Walsall Healthcare NHS Trust processes personal information regarding individuals (*data subjects*), we are obligated under the GDPR to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR and its principles.

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; 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."

Walsall Healthcare NHS Trust ensures that even greater care and attention is given to personal data falling within the GDPR's ***'special categories'*** *(previously referred to under the DPA as* ***sensitive personal data****)*, due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -
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 shall be prohibited – unless one of the Article 9 clauses applies.

The GDPR regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating or destroying any such data.

As Walsall Healthcare NHS Tust uses personal data in one or more of the above capacities, we have put into place robust measures, policies, procedures and controls concerning all aspects of personal data handling.

We are proud to operate a 'Privacy by Design' approach and aim to be proactive not reactive; assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2. Scope

The policy relates to all staff (including permanent, fixed term, temporary, third-party representatives or sub-contractors, agency workers, volunteers and students 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 ensure that Walsall Healthcare NHS Trust is meeting its legal, statutory and regulatory requirements under the GDPR and to ensure that all personal and special category information is safe, secure and processed compliantly whilst in use and/or being stored and shared by us.

The Trust is dedicated to compliance with the GDPR's principles and understands the importance of making personal date safe within our organisation.

The GDPR 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.

The GDPR Principles

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the GDPR principles'* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

The Information Commissioners Office (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 1998 *(pre-25th May 2018) (update with new DP law once passed)*
- General Data Protection Regulation *(post-25th May 2018)*
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the GDPR the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as before when it comes to oversight, enforcement and responding to complaints with regards to the GDPR and those firms located solely in the UK.

However, where an organisation is based in more than one Member State and/or where cross border processing takes place, a lead Supervisory Authority will enforce the GDPR requirements in consultation with any associated Supervisory Authority. Under the GDPR, the *'lead'* is determined by the location of the *'main establishment'*.

Walsall Healthcare NHS Trust are registered with ICO and appear on the Data Protection Register as a [controller and processer] of personal information.

Our Data Protection Registration Number is Z5161445.

Penalties

Walsall Healthcare NHS Trust understands our obligations and responsibilities under the GDPR and Supervisory Authority and comprehends the severity of any breaches under the Regulation.

We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that: -

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Objectives

We are committed to ensuring that all personal data obtained and processed by Walsall Healthcare NHS Trust is done so in accordance with the GDPR and its principles, along with any associated regulations and/or codes of conduct laid out by the Supervisory Authority and local law.

We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to uphold the highest standards of data processing.

Walsall Healthcare NHS Trust uses the below objectives to meet the regulatory requirements of the GDPR and to develop measures, procedures and controls for maintaining and ensuring compliance.

Walsall Healthcare NHS Trust ensures that: -

- We protect the rights of individuals with regards to the personal information known and held about them by in the course of our business.
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the GDPR.
- Every business practice, task and process carried out is monitored for compliance with the GDPR and its principles.
- Data is only obtained, processed or stored when we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
- All employees (*including new starters and agents*) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the GDPR principles, regulations and how they apply to our business and services.
- Patients, service users and members of staff feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the GDPR.
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the GDPR and to identify gaps and non-compliance before they become a risk.
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news and updates, to stay abreast of updates, notifications and additional requirements.
- We have robust and recorded Complaint Handling and Breach Incident controls and procedures in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision and implementation of the GDPR and its principles and remains informed on the regulations and how they relate to us.
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program utilises this policy and procedure and the GDPR itself to ensure continued compliance.
- We provide clear lines of reporting and supervision with regards to data protection compliance.
- Develop and maintain strict and robust DPA procedures, controls and measures to ensure continued compliance with the Act.

- We store and destroy all personal information, in accordance with the GDPR timeframes and requirements.
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their own rights under the GDPR and are provided with the Article 13 & 14 information disclosures

4. Roles and responsibilities

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

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.

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 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

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

Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by Walsall Healthcare NHS Trust we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing.

We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the GDPR and any codes of conduct that we have obligations under.

We can demonstrate that all processing activities are performed in accordance with the GDPR and that we have in place robust policies, procedures, measures and controls for the protection of data.

We operate a transparent workplace and work diligently to guarantee and promote a comprehensive and proportionate governance program.

Our main governance objectives are to*:* -

- Educate senior management and employees about the requirements under the GDPR and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all staff

- Identify key senior stakeholders to support the data protection compliance program

- Allocate responsibility for data protection compliance and ensure that the designated person has sufficient access, support and budget to perform the role

- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that Walsall Healthcare NHS Trust has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies (*i.e. Information Management and Technology Policy, Safe Haven Policy, Incident Management Policy).*

Privacy by Design

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities.

We therefore have additional measures in place to adhere to this ethos, including: -

Data Minimisation
Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep if for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose.

Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the GDPR.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain

- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected

- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor).* These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Pseudonymisation
We utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (*personal identifiers*).

Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation means that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format.

Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities.

Restricting access is built into the foundation of Walsall Healthcare NHS Trust's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and should only be accessed by those with a legitmate interest.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of patient records, hospital invoices or claims information*).

Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for.

Steps include: -

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject.

- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*).

- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (*i.e. we do not use the postal system as this can be intercepted*).

- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked.

- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key.

- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the GDPR*), we destroy the hard copy data and delete the sent message.

- If for any reason a copy of the paper data must be retained we will save them in a secure manner.

Information Flow Audit

To enable Walsall Healthcare NHS Trust to fully prepare for and continue to comply with the GDPR, we have carried out a Trust-wide data protection information flow assessment to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our company in our capacity as a controller/processor and has been compiled on a central register which 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?

- Disclosures and Transfers

The audit will be conducted on an annual basis by the Compliance and Risk Team/Data Protection Officer.

Lawfulness of Processing

At the core of all personal information processing activities undertaken by Walsall Healthcare NHS Trust is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations.

Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information flow register and where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes

- 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

- Processing is necessary for compliance with a legal obligation to which we are subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Walsall Healthcare NHS Trust

- Processing is necessary for the purposes of the legitimate interests pursued by Walsall Healthcare NHS Trust 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).*

Records of Processing Activities

As an organisation with *more than* 250 employees, Walsall Healthcare NHS Trust maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

Acting in the capacity as a controller *(or a representative*), our internal records of the processing activities carried out under our responsibility, contain the following information: -

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative

- The purposes of the processing

- A description of the categories of data subjects and of the categories of personal data

- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations)

- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)

- Where possible, the envisaged time limits for erasure of the different categories of data

- A general description of the processing security measures as outlined in section 12 of this document (pursuant to Article 32(1) of the GDPR)

Acting in the capacity as a processor (*or a representative*), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information: -

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer

- The categories of processing carried out on behalf of each controller
- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)

- A general description of the processing security measures as outlined in section 13 of this document (pursuant to Article 32(1) of the GDPR)

Third-Party Processors

Walsall Healthcare NHS Trust utilise external processors for certain processing activities.

We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible.

Such external processing includes (but is not limited to): -

- Legal Services
- Text Messaging Reminder Services

The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the GDPR even when a process is handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists Walsall Healthcare NHS Trust in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments

- When requested, deletes or returns all personal data to Walsall Healthcare NHS Trust after the end of the provision of services relating to processing, and deletes existing copies where possible

- Makes available to Walsall Healthcare NHS Trust all information necessary to demonstrate compliance with the obligations set out here and in the contract

- Allows and supports audits, monitoring, inspections and reporting as set out in the contract

- Informs Walsall Healthcare NHS Trust immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

Data Retention & Disposal

Walsall Healthcare NHS Trust have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary.

All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and priorities the protection of the personal data at all times.

Please refer to our Records Retention Policy for full details on our retention, storage, periods and destruction processes.

Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected at all times whilst their data is being stored and processed by Walsall Healthcare NHS Trust.

We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where Walsall Healthcare NHS Trust must or is considering carrying out processing that utilises new technologies, where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessments (DPIA) (sometimes referred to as a Privacy Impact Assessment).

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

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach an allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and protection the privacy and impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

Refer to the Data Protection Impact Assessment standard operating procedure.

Data Subject Rights Procedures

Consent and the Right to be Informed

Consent for the processing of information for **direct health care purposes** is **not required** under the following article:

Article 9(2)(h) – the processing is necessary for the purpose of medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems.

However, where consent is required for processing we have specific measures and controls in place to ensure that we comply with the conditions for consent under the GDPR.

The GDPR defines consent 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'.*

Where processing is based on consent, Walsall Healthcare NHS Trust has reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms

- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes

- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data

- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand

- Pre-ticked, opt-in boxes are **never** used

- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is **not** a precondition of any service (unless necessary for that service)
- Along with our Trust's name, we also provide details of any other third party who will use or rely on the consent

- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case

- We keep detailed records of consent and can evidence at a minimum:-
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our Trust's name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained

- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email

- Consent withdrawal requests are processed immediately and without detriment

- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent

- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents

- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

Consent Controls

Walsall Healthcare NHS Trust maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.
The GDPR states that where processing is based on consent and the personal data relates to a child who is below the age of 16 years, such processing is only carried out by Walsall Healthcare NHS Trust where consent has been obtained by the holder of parental responsibility over the child.

The UK's Data Protection Bill reduces this age to *13 years*, as per Article 8(1) of the GDPR what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

Consent to obtain, process, store and share (*where applicable*), is obtained by Walsall Healthcare NHS Trust through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Points 1-4 are enforced using scripts, checklists, on-screen prompts and signed customer agreements, to ensure that consent has been obtained and to remind employees of their additional consent obligations, as below.

Electronic consent is always a double opt-in, enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent to ensure that we are compliant in disclosing the information required in the GDPR in an easy to read and accessible format.

Alternatives to Consent

Walsall Healthcare NHS Trust recognise that there are six lawful bases for processing and that consent is not always the most appropriate option.

We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent, but would still process it even if it was not given (or withdrawn). If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use

- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate

- Where there is an imbalance in the relationship, i.e. with employees

Information Provisions

Where personal data is obtained directly from the individual (i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc)), we provide the below information in all instances, in the form of a consent/privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that Walsall Healthcare NHS Trust intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where Walsall Healthcare NHS Trust intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards Walsall Healthcare NHS Trust has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

Privacy Notices

Where Walsall Healthcare NHS Trust obtains personal data from a data subject or a third-party, we utilise Privacy Notices to provide the information.

Our privacy notice is easily accessible, legible, jargon-free and inclusive of all information and is available in several formats as applicable to the method of data collection: -

- Via our website
- Linked to or written in full in the footer of emails
- In our Privacy Policy
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Via SMS
- Printed media and adverts

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

Personal Data Not Obtained from the Data Subject

Where Walsall Healthcare NHS Trust obtains and/or processes personal data that has not been obtained directly from the data subject, Walsall Healthcare NHS Trust ensures that the relevant information is provided to the data subject within 30 days of our obtaining the personal data (except for advising if the personal data is a statutory or contractual requirement).

In addition to the information provided to the data subject, we also provide information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where Walsall Healthcare NHS Trust intends to further process any personal data for a purpose *other* than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information to data subjects, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which Walsall Healthcare NHS Trust is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

Employee Personal Data

As per the GDPR guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information.

Our Human Resource policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the GDPR and how to exercise these rights.

The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request was received.

Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary.

However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by Walsall Healthcare NHS Trust from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the SARs team as soon as received and a record of the request is noted. The type of personal data held about the individual is checked to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge, unless the request is deemed as manifestly unfounded or excessive (see Patient Records Policy).

Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our Patient Records Policy for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the GDPR.

Data Portability

Walsall Healthcare NHS Trust provides all personal information pertaining to the data subject, to them on request and in a format, that is easy to disclose and read.

We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the GDPR concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from Walsall Healthcare NHS Trust to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML
- CSV
- XML
- RDF
- XHTML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received.

If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

Rectification & Erasure

Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by Walsall Healthcare NHS Trust is reviewed and verified as being accurate wherever possible and is always kept up to date.

Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

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.

The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

The Right to Erasure

Also, known as *'The Right to be Forgotten'*, Walsall Healthcare NHS Trust complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by Walsall Healthcare NHS Trust is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where Walsall Healthcare NHS Trust has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

Such refusals to erase data include: -

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

The Right to Restrict Processing

There are certain circumstances where Walsall Healthcare NHS Trust restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request.

Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

Walsall Healthcare NHS Trust will apply restrictions to data processing in the following circumstances: -

- Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties.

Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed.

We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notice.

We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. *Individuals have the right to object to: -*

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where Walsall Healthcare NHS Trust processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*.

We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, Walsall Healthcare NHS Trust will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention.

We also assess new systems and technologies for this same component prior to implementation. Walsall Healthcare NHS Trust understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the GDPR, we aim to put measures into place to safeguard individuals where appropriate.

Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, Walsall Healthcare NHS Trust will use automated decision-making processes within the guidelines of the regulations.

Such instances include: -

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where Walsall Healthcare NHS Trust uses automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

Oversight Procedures

Security & Breach Management

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

Our Information Management and Technology Policy, Safe Haven Policy and Records Retention Policy provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

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 and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure is taken to reduce the risk of data breaches, Walsall Healthcare NHS Trust has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our Data Breach Standard Operating Procedure for further information.

Passwords

Passwords are a key part of Walsall Healthcare NHS Trust's protection strategy and are used throughout the Trust to secure information and restrict access to systems.

We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Whilst passwords are also directly related to Information Security and Access Control, Walsall Healthcare NHS Trust recognises strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password.

Full procedures and guidelines for passwords, access and security can be found in our Information Management and Technology Policy.

Restricted Access and Clear Desk Policy

Walsall Healthcare NHS Trust may on occasions and at its discretion, place all or part of its files onto a secure computer network with restricted access to all/some personnel data.

When implemented, access to personal information will only be granted to the person/department that has a specific and legitimate purpose for accessing and using such information.

Walsall Healthcare NHS Trust operates a zero-tolerance Clear Desk Policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers etc.

Access to areas where personal information is stored (both electronic and physical) are on a restricted access basis with secure controlled access functions throughout the building.

Only staff authorised to access data or secure areas can do so. All personal and confidential information in hard copy is stored safely and securely.

Transfers and Data Sharing

Walsall Healthcare NHS Trust takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the GDPR covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and all data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

We conduct transfers of personal data to third countries or international organisations where the Commission has advised that adequate levels of protections are in place. Such transfers are reviewed by the DPO and carried out following the same process as those within the EU. The DPO is responsible for monitoring the approved third country list provided by the

Commission and only transferring data under this provision to those countries, organisations or sectors listed.

Appropriate Safeguards

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organisation, we restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject.

In such instances, we develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organisation.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and that effective legal remedies for data subjects are available.

The appropriate safeguards can be provided without Supervisory Authority authorisation by: -

- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights

With authorisation from the Supervisory Authority, the appropriate safeguards may also be provided for by: -

- Contractual clauses between Walsall Healthcare NHS Trust and the controller, processor or the recipient of the personal data in the third country or international organisation
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

Walsall Healthcare NHS Trust does not transfer personal data to any third country or international organisation without one or more of the above safeguards being in place or without the authorisation of the Supervisory Authority where applicable.

We verify that any safeguards, adhere to the GDPR Principles, enforce the rights of the data subject and protect personal information in accordance with the Regulation.

Pursuant to Article 46, we ensure that any agreement, contract or binding corporate rules for transferring personal data to a third country or international organisation, are drafted in accordance with any Supervisory Authority and/or the Commission's specification for format and procedures (where applicable).

As a minimum standard, we verify that the below are specified: -

- The structure and contact details of the group engaged in the activity and of each of its members
- The data transfers or set of transfers, including: -
    - the categories of personal data
    - the type of processing and its purposes
    - the type of data subjects affected
- the identification of the third country or countries in question
- Their legally binding nature, both internally and externally
- The application of the general data protection principles, in particular: -
    - purpose limitation
    - data minimisation
    - limited storage periods
    - data quality
    - data protection by design and by default
    - legal basis for processing
    - processing of special categories of personal data
    - measures to ensure data security
    - the requirements in respect of onward transfers to bodies not bound by the binding corporate rules
- The rights of data subjects regarding processing and the means to exercise those rights, including the right: -
    - not to be subject to decisions based solely on automated processing (inc profiling)
    - to lodge a complaint with the competent Supervisory Authority and before the competent courts of the Member States
    - to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules
- Our acceptance (*and that of any processor acting on our behalf*) of liability for any breaches of the binding corporate rules by the third country or international organisation to whom the data is being transferred (with exemption from that liability, in whole or in part, only where we prove that we are not responsible for the event giving rise to the damage)
- How the information on the binding corporate rules and the information disclosures (Articles 13 & 14) is provided to the data subjects (with particular reference to the application of the GDPR Principles, the data subjects rights and breach liability)
- The tasks of any Data Protection Officer and/or person(s) in charge of monitoring compliance with the binding corporate rules, as well as monitoring training and complaint-handling
- The complaint procedures
- The mechanisms within the group engaged in the activity, for ensuring the verification of compliance with the binding corporate rules, including: -

  - data protection audits
  - methods for ensuring corrective actions to protect the rights of the data subject
  - providing the Data Protection Officer and controlling board with such verification results
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the Supervisory Authority
- The cooperation mechanism with the Supervisory Authority to ensure compliance by any member of the group, in particular by making available to the Supervisory Authority, the results of verifications of the measures referred to above
- The mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules
- The appropriate data protection training to personnel having permanent or regular access to personal data

Transfer Exceptions

Walsall Healthcare NHS Trust does not transfer any personal information to a third country or international organisation without an adequacy decision by the Commission or with Supervisory Authority authorisation and the appropriate safeguarding measures; unless one of the following conditions applies.

The transfer is: -

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards
- necessary for the performance of a contract between the data subject and Walsall Healthcare NHS Trust or the implementation of pre-contractual measures taken at the data subject's request
- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between Walsall Healthcare NHS Trust and another natural or legal person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register). Transfer made under this exception must not involve the entire personal data or categories of the personal data in the register and if the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer is not valid under Article 45 or 46 and none of the above derogations apply, Walsall Healthcare NHS Trust complies with the Article 49 provision that a transfer

can still be affected to a third country or an international organisation where all the below conditions apply.

The transfer: -

- cannot be made by a public authority in the exercise of its public powers
- is not repetitive
- concerns only a limited number of data subjects
- is necessary for the purposes of compelling legitimate interests pursued by Walsall Healthcare NHS Trust which are not overridden by the interests or rights and freedoms of the data subject
- Walsall Healthcare NHS Trust has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data

[NOTE: The first three derogations are not available for the activities of public authorities in the exercise of their public powers.]

Where the above transfer must take place for legal and/or compelling legitimate reasons, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures pursuant to Articles 13 and 14, as well as being informed of the transfer, the compelling legitimate interests pursued and the safeguards utilised to affect the transfer.

6. Audit / monitoring arrangements

This policy and procedure document details the extensive controls, measures and methods used by Walsall Healthcare NHS Trust to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the GDPR and associated laws and codes of conduct.

In addition to these, we also carry out regular audits and compliance monitoring processes that are detailed in our General Data Protection Regulation Audit Checklist, Appendix 1, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable.

Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

Monitoring Process	Requirements
Who	Governance Department
Standards Monitored	• Ensure that the appropriate policies and procedures are in place; • To verify that those policies and procedures are being followed; • To test the adequacy and effectiveness of the measures and controls in place; • To detect breaches or potential breaches of compliance; • To identify risks and assess the mitigating actions in place to minimise such risks; • To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data; • To monitor compliance with the GDPR and demonstrate best practice.
When	Annually
How	• Audits • Risk Management: Review of Risks/Action Plan • Incident Reporting
Presented to	Information Governance Steering Group
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 in the EU who, 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 i.e. Information Commissioner's Office.

Binding Corporate Rules means personal 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

Data Breach Policy and 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 - The Audit Checklist

This GDPR Audit Checklist has been developed for dual purpose and can be used as an audit and progress tool prior to the GDPR coming in to effect; to check existing measures and controls against the GDPR requirements and obtain a working action plan for what needs addressing and putting into place. It can also be used after 25th May 2018, when the GDPR is in force, to assess ongoing compliance and meet the audit requirements for demonstrating that processes, controls and measures are regularly assessed and reviewed against the GDPR requirements.

Two versions of the checklist are available, both providing the same questions, but offering slightly different user experiences.

Word Version
This version of the audit checklist can easily be printed out before and after the checklist process and enables hard copy auditing across the business. It is effective for those who prefer a written assessment and to have physical pages to look back over when assessing gaps and adding notes.

Excel Version
The Excel format has duplicated questions, but also uses a drop-down feature for noting whether you are fully, partially or not compliant with the criteria questions; and offers the useful ability of being able to filter the table columns so that you can select just those areas where improvements need to be made.

Using the Audit Checklists

The checklist covers every aspect of the data protection standards and requirements and can be used to review, assess and improve the measures and controls that you have in place to protect data subjects, their rights and their personal information.

You should assess all business areas and process with each question and only answer yes where you are already fully compliant with the GDPR. The notes section can be used to make notes on gaps, improvements or for areas that are not applicable to your organisation.

You should also use the review date section for when an item is added to your action plan for follow up and can be re-assessed on the checklist. Some of the questions relate to specific Articles & Recitals in the Regulation. Where there is an associated Article/Recital, these are noted to the left of each question.

Action Plan

Once you have completed the audit, you should use the action plan template to detail gaps and areas of non-compliance, then add actions and dates for implementing processes, systems or controls that will comply with the standards or requirements. Action plans and completed audits should be retained for 6 years and be made available to the Supervisory Authority upon request.

GENERAL DATA PROTECTION REGULATION AUDIT CHECKLIST		
LEAD AUDITOR:		***DIRECTIONS:*** *1. Answer each requirement based on your current process* *2. Refer to the relevant GDPR Article if you need further clarification on meeting the standard or requirement (if the question relates to a specific Article, it is noted to the left of the question – those without Article references are suggested requirements or guidelines from the ICO or WP29)* *3. Use the requirement number on the Action Plan where corrective actions or mitigating controls are required* *4. Where actions are needed, add a review date for re-auditing*
AUDIT DATE:		
AUDIT DESCRIPTION:		

1. GOVERNANCE & ACCOUNTABILITY								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
1.1	24	78	Do you have a Data Protection Policy?					
1.2			Do you have a Clear Desk Policy?					
1.3			Do you have a Remote Access Policy?					
1.4	24	78	Do you have Data Breach Incident & Notification Policy & Procedures?					
1.5	24	78	Do you have a Records Management & Data Retention Policies?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
1.6		78	Do you have an Information Security Policy?					
1.7			Do you have a documented Business Continuity Plan?					
1.8			Do you have documented procedures for obtaining, processing					

			& storing personal data?					
1.9	24, 25, 28, 32	74, 77, 78, 81, 83	Have you implemented appropriate technical and organisational measures to protect data & reduce risks?					
1.10			Have you conducted an Information Audit?					
1.11			***Does your Information Audit contain: -*** • What personal data you hold? • Where it came from? • Who you share it with? • Legal basis for processing it? • What format(s) is it in? • Who is responsible for it?					
1.12	4, 24, 28	74, 81	Have you assessed and documented whether you are a *'Data Controller'*, *'Data Processor'* or both?					
1.13	25, 40, 42, 43	98, 99, 100	If you have obligations under any data protection Codes of Conduct or Certifications, do you disseminate these codes/requirements to all staff?					
1.14			Have your HR policies and procedures been reviewed *(and if applicable, revised)* to ensure that employee's individual rights under the GDPR are considered and complied with?					
2. DATA PROTECTION OFFICER (DPO)								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
2.1	37	97	Have you allocated responsibility for data protection compliance to a designated person (i.e. *DPO or suitable individual*)?					
2.2	38	97	Does the Data Protection Officer (DPO) have sufficient access,					

			support and the budget to perform the role?					
2.3	38	97	Has the DPO identified, created and disseminated reporting lines for the data protection governance structure?					
2.4	38	97	Are all employees aware of the DPOs appointment & contact details?					
2.5	38	97	If the DPO has other tasks and duties, have they been assessed to ensure there is no conflict of interest?					
2.6	37, 39	97	Has the DPO been assessed & verified as having adequate professional qualities and expert knowledge of data protection and the ability to fulfil the tasks referred to below? • To inform and advise the business, management, employees & third parties who carry out processing, of their obligations under the GDPR • To monitor compliance with the GDPR and with the firm's own data protection objectives • Assignment of responsibilities, awareness-raising and training of staff involved in processing operations • To provide advice where requested as regards the data protection impact assessment and monitor its performance • To cooperate with the Supervisory Authority • To act as the contact point for the Supervisory Authority on issues relating to processing					
2.7	38	97	Is the DPO bound by secrecy and/or confidentiality?					
2.8	37	97	Have you published the contact details of the Data Protection Officer?					

2.9	37	97	Have the DPO's contact details been communicated to the Supervisory Authority?					
2.10	38	97	Does the DPO have access to suitable training materials, courses and workshops to support and improve their role & knowledge?					
2.11			Have reporting mechanisms been developed between the DPO and senior management?					
3. PRIVACY BY DESIGN & SECURE PROCESSING								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
3.1			Are daily data backups performed and all back-ups kept in a secure, restricted access location?					
3.2	24, 25, 28, 32	28,29, 78, 83	Do you utilise pseudonymisation and/or encryption methods to secure personal data?					
3.3	24, 25, 28, 32	28,29, 78, 83	Do you ensure that pseudonyms and their personal identifiers and/or encryption methods and their secret keys, are always kept separate and secure?					
3.4	25	78	Do you advocate data minimisation & only obtaining and processing the minimum information necessary for the purpose specified?					
3.5	25	78	Is data collected by electronic means (*i.e. forms, website, surveys etc*) minimised so only the relevant fields are used, as relevant to the processing purpose?					
3.6	24, 25	78	Do you have documented destruction procedures in place for information that is no longer necessary, surplus to requirement or part of an individual's consent withdrawal or right to erasure?					

3.7	24, 25	78	If you must use hard copy data for storing or processing, do you use redaction methods where possible to ensure data minimisation?					
3.8			Do you enforce strong passwords across your organisation?					
3.9			Are passwords to networks, computers and backups changed every 30 days?					
3.10	24, 25	78	Do you restrict access to personal information to only those employees processing the data?					
3.11	25, 32	78, 83	Do you activate strong security defaults on all systems and networks?					
3.12	32	83	Do you carry out frequent audits & reviews to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?					
3.13			Do you have documented; robust & tested business continuity plans to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident?					
3.14	24, 25, 32	83	Do you have a documented audit & review process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing?					
4. PRINCIPLES & PROCESSING ACTIVITIES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
4.1	5	39, 60	***Is personal information: -*** • processed lawfully, fairly and in a transparent manner?					

			• collected for specified, explicit and legitimate purposes only? • adequate, relevant and limited to what is necessary? • accurate and, where necessary, kept up to date • kept only for as long as is necessary and only for the purpose(s) which it is processed? • processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage?					
4.2	32	75, 76, 77	Have you carried out a risk assessment to identify, assess, measure and monitor the impact(s) of processing?					
4.3	30, 32	82	Do you carry out internal audits of all processing activities?					
4.4	6	40-50	Do you identify and establish the legal basis for all personal data that you process?					
4.5	9	51-56	If you process special category, is it in compliance with one or more of the Article 9(2) conditions?					
4.6a	30	13, 82	***If you employee <u>less</u> than 250 people, do you maintain records of all processing activities where: -*** • Processing personal data could result in a risk to the rights and freedoms of individual? • The processing is not occasional? • You process special categories of data or criminal convictions and offences?					
4.6b	30	82	***If you employee <u>more</u> than 250 people and act in the capacity as a <u>controller</u> (or a representative), do your internal records of***					

			the processing activities carried contain: - • Your full name and contact details and the name and contact details of the Data Protection Officer? • Where applicable, details of any joint controller and/or the controller's representative? • The purposes of the processing? • A description of the categories of data subjects and of the categories of personal data? • The categories of recipients to whom the personal data has or will be disclosed *(including any recipients in third countries or international organisations*)? • Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)? • Where possible, the envisaged time limits for erasure of the different categories of data? • A general description of the processing security measures you have in place?					
4.6c	30	82	***If you act in the capacity as a <u>processor</u> (or a representative) <u>on behalf of a controller</u>, do your internal records of the categories of processing activities carried out, contain: -*** • Your full name and contact details? • The full name and contact details of each controller on behalf of which you are acting? • The name and contact details of the Data Protection Officer?					

			• The categories of processing carried out on behalf of each controller • Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)? • A general description of the processing security measures you have in place?					
4.7	30	82	***Do you ensure that the above records are: -*** • maintained in writing? • provided in a clear and easy to read format? • readily available to the Supervisory Authority upon request?					
4.8	6	40-50	Prior to obtaining & processing personal information, do you carry out a review to verify compliance with one or more of the lawfulness of processing conditions?					
5. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
5.1	35	84, 90	When processing is likely to be high risk or cause significant impact to a data subject, do you carry out Data Protection Impact Assessments (DPIA)?					
5.2	35	84, 90	Do you have a process and screening questions for determining whether a DPIA is required?					
5.3	35	84, 90	Does this process utilise the Article 35 definitions of high risk processing?					

5.4	24		Do you have documented policies & procedures for completing a DPIA?					
5.5	35, 39		Is the DPO always involved in the assessment and mitigating action plan?					
5.6	35	90	***Does the DPIA contain: -*** • A systematic description of the envisaged processing operations? • The purposes of the processing? • Where applicable, the legitimate interest pursued by the controller? • An assessment of the necessity and proportionality of the processing operations in relation to the purposes? • An assessment of the risks to the rights and freedoms of data subjects? • The measures envisaged to address the risks *(inc. safeguards, security measures and mechanisms to ensure the protection of personal data)*?					
5.7	35		Where appropriate, do you seek the views of data subjects or their representatives on the intended processing?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
5.8	35, 36	90	Are mitigating measures proposed & actioned to reduce the impact of the risk?					
5.9			Are all DPIAs documented in writing?					
5.10	35		Where there is a change to the risk posed by processing, is a review of the DPIA carried out?					

5.11	36	94, 96	Where measures fail, or cannot mitigate the risk, do you consult the Supervisory Authority prior to processing where a DPIA indicates that the processing would result in a high risk?					
5.12	36	94, 96	***If consulting the Supervisory Authority, do you provide: -*** • The respective responsibilities of the controller *(if applicable*)? • Joint controllers and processors involved in the processing *(if applicable)?* • The purposes and means of the intended processing? • The measures and safeguards provided to protect the rights and freedoms of data subjects? • The contact details of the Data Protection Officer? • The data protection impact assessment? • Any other information upon request?					
6. CONSENT & INFORMATION DISCLOSURES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.1	7	32, 42, 43	Are you always able to demonstrate that consent has been given?					
6.2	7, 12	32, 42, 60	Where processing is based on consent, is the request in a clear and transparent format, using plain language and avoiding any illegible terms or jargon?					
6.3	7, 12	42	Is the request in an easily accessible format with the purpose for data processing attached to that consent?					

6.4	7	42	Where consent is requested in the context of a written declaration which also concerns other matters, is the request always presented in a manner which is clearly distinguishable from the other matters?					
6.5	7, 17	42, 65	Is the data subjects' right to withdraw consent at any time made clear?					
6.6	7	42, 65	Is the process for withdrawing consent simple, accessible and quick?					
6.7	8	38	Where personal information is obtained and/or processed relating to a child under 16 years (***13 years for DP Bill in UK***), do you ensure that consent is given and documented by the holder of parental responsibility over the child?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.8	8, 12	38, 58	Where services are provided to children, does your communication information and privacy notice provide clear & plain information that is easy to understand by a child?					
6.9			When physically collecting personal information (*i.e. face-to-face, telephone etc*), are supporting scripts used to remind staff of the conditions for consent and an individual's right to be informed?					
6.10	7		Do you have clear audit trails to evidence consent and where it came from?					
6.11	13, 14	42, 60, 61	Do you utilise a Privacy Notice/Policy (*on your website, contracts, emails etc*) to ensure compliance with the conditions for consent and information disclosure rules?					

6.12	13	42, 60, 61	***Where personal data is <u>collected directly</u> from the data subject, do you ensure that the below information is provided at the time of consent: -*** • Identity and contact details of the controller (*or controller's representative)?* • Contact details of the Data Protection Officer? • Purpose of the processing and the legal basis for the processing? • The legitimate interests of the controller or third party? • Any recipient or categories of recipients of the personal data? • Details of transfers to third country and safeguards? • Retention period or criteria used to determine the retention period? • The existence of each of data subject's rights? • The right to withdraw consent at any time, where relevant? • The right to lodge a complaint with a supervisory authority? • Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data? • The existence of automated decision making (*inc profiling*) & information about the logic involved & the significance/envisaged consequences for the data subject?					

6.13	14	61	***Where personal data has <u>not</u> been obtained directly from the data subject, do you ensure, in addition to the above disclosures, that you also provide: -*** • The categories of personal data? • The source the personal data originates from and whether it came from publicly accessible sources?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
6.14			Do you test, review & audit Privacy Notices to ensure adequacy, effectiveness and data subject understanding?					
6.15			Are final Privacy Notices authorised by Senior Management/Director and the DPO before being activated?					
6.16	7, 13, 14	32	Is the Privacy Notice displayed clearly and prominently?					
6.17	7, 13, 14	32	Are individuals asked to positively opt-in?					
6.18	7, 13, 14	32	Does the Privacy Notice give the individual sufficient information to make an informed choice?					
6.19	7, 13, 14	32	Does the Privacy Notice explain the different ways that you will be using the personal information?					
6.20	7, 13, 14	32, 60	Have you provided a clear and simple way for individuals to indicate that they agree to different types of processing?					
6.21	7, 13, 14	32	Does the Privacy/Consent Notice include a separate unticked opt-in box for direct marketing?					

6.22	6, 7, 13, 14	32	Does your Privacy Notice clearly define the lawful basis for processing?					
7. DATA SUBJECT NOTIFICATIONS, REQUESTS & COMMUNICATION								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
7.1	12	60	Where you act on a data subjects request under Articles 15 to 22, do you provide information on the actions taken in writing *(i.e. data erasures, rectifications etc)*?					
7.2	12	58, 60	For information disclosures (*Articles 13 & 14*) and communications relating to Articles 15-22 & 34, are responses and information sent to individuals in a concise, transparent, intelligible and easily accessible form?					
7.3	12	59	Is requested/required information sent free of charge (*unless a specific GDPR requirement states otherwise*)?					
7.4	12	59	Is requested/required information sent within 30 days of receiving the data subjects' request/action?					
7.5	12	59	Where it is not possible to comply with the 30-day timeframe for responding, do you inform the data subject(s) of the extension within 30 days of receipt of the request, together with the reasons for the delay?					
7.6	12	59	If you do not act on a request under a right exemption, do you inform the data subject within 30 days, of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy?					
7.7	12	58, 60	Where communicating with a data subject, is the content always					

			clear and using plain language?					
7.8	12	58, 60	When requesting access to information or exercising a right, is the information provided to the individual in writing and/or by electronic means (*where appropriate*)?					
7.9	12	64	If the data subject requests access to processing information and this is to be provided orally, do you verify the individual's identity by other means first?					
7.10			Have you reviewed all existing data subject request processes and timeframes and updated them to comply with the new deadlines and GDPR timeframes?					
7.11	12, 15	59, 63	Do you have dedicated procedures for handling subject access requests and request refusals?					
8. DATA SUBJECT RIGHTS								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
8.1	15	63, 64	***Where a data subject exercises their Right of Access, do you ensure that they are provided with: -*** • The purposes of the processing? • The categories of personal data concerned • The recipients or categories of recipient to whom the personal data has/will be disclosed? • Whether the personal data has/will be transferred to a third countries or international organisations? • Pursuant to the above, the right to be informed of the appropriate safeguards used?					

			• The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period? • The existence of the right to request rectification or erasure of personal data? • The existence of the right to restrict processing of personal data or to object to such processing? • The right to lodge a complaint with a supervisory authority? • Where the personal data was not collected directly from the data subject, information as to the source? • The existence of automated decision-making *(inc. profiling*) and details of the logic involved, as well as any significant/envisaged consequences of such processing?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
8.2	16	65	Do you have a process for rectifying inaccurate personal data and/or completing incomplete personal data completed *(inc supplementary statements*)?					
8.3	17	65, 66	***Where a data subject exercises their Right to Erasure, do you check the request against the below list before complying?*** • The personal data is no longer necessary in relation to the purposes for which it was collected. • The data subject withdraws consent on which the processing is based. • The personal data has been unlawfully processed. • The personal data must be erased for compliance with a					

			legal obligation. • The personal data has been collected in relation to the offer of information society services. • The data subject objects, on grounds relating to their particular situation, to processing of concerning them which is based on points (e) or (f) of Article 6(1). • The data subject objects to the processing pursuant to data being processed for direct marketing purposes.					
8.4	17	65, 66	Where the data subject has a valid request to have personal data erased and that data has been made public, do you take every reasonable step, to request the erasure by such controllers of any links to, or copy or replication of, those personal data?					
8.5	18	67	Where the accuracy of the personal data has been contested by the data subject, do you restrict processing for a period to enable verification of the accuracy of the personal data?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
8.6	18	67	Where processing is no longer necessary or lawful, do you have a process for restricting processing where requested this over erasure?					
8.7	19	66	Do you notify any third party also processing such information about the restriction? *(using the data from your Information Audit)*					
8.8	21		Where a data subject exercises rights of erasure, objection or rectification, do you restrict processing for a period to enable verification of the validity of the request?					
8.9	18	67	Do you ensure that where a data subject has obtained					

			restriction of processing, they are informed in writing before the restriction is lifted?					
8.10	20	68	Where possible, do you retain copies of personal data in a structured, commonly used and machine-readable format to comply with the Right to Data Portability?					
8.11	20	68	If requested by a data subject, do you transmit personal data to another controller in a machine-readable format?					
8.12	22	71, 72	Do you avoid using solely automated processing (*inc profiling*) in your decision-making processes, unless consent has been given by the data subject?					
8.13	12	59	Do you have procedures and controls in place to ensure that all personal information can be provided electronically?					
8.14	21	70	Can individuals object to having their personal information processed for direct marketing?					
9. TRANSFERS, SHARING & THIRD PARTIES								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.1	28	81	If you use a third party to process any personal information (*e.g. I.T Services, HR Providers etc*), do you carry out due diligence checks prior to selection?					
9.2	28, 32	81	***Do you have compliant Service Level Agreements (SLAs) and contracts with each third party processor, which outline: -*** • Required skill, competency and knowledge? • The processors data protection obligations? • Your expectations, rights and obligations? • The processing duration, aims and objectives?					

			• The data subjects' rights and safeguarding measures? • The nature and purpose of the processing? • The type of personal data & categories of data subjects? • Frequency & type of ongoing due diligence & monitoring?					
9.3	28, 32	81, 83	When transferring or disclosing personal information, do you encrypt the data and only send what is necessary?					
9.4	32		Do you use secure data transfer methods for communications (*i.e. emails, website forms, online payments*)?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.5	28, 32	78, 79, 81, 83	***When sharing or disclosing personal information, do you carry out a data sharing assessment and identify and record: -*** • The benefits and risks of sharing the data • The objectives and goal of sharing • What information needs to be shared • Who requires access to the shared personal data • How should it be shared • Encryption methods and data minimisation tools • How to assess and monitor that the sharing is achieving its objectives? • Due diligence checks of the entity or individual who will receive the personal information?					
9.6			Is the DPO (*or appointed suitable individual*) and I.T Manager/Department involved in the setup of any personal data transfers?					

9.7	45, 46, 47, 48	101-107	**Do you only effect a transfer of personal data to a third country or international organisation (*outside of the EU*), where one or more of the below conditions applies?** **1.** Where the Commission has decided that the third country/organisation ensures an adequate level of protection (*Adequacy Decision)* **2.** In the absence of an Adequacy Decision, where you have provided appropriate safeguards and have ensured that enforceable data subject rights and effective legal remedies for data subjects are available **3.** With Supervisory Authority authorisation, transfers can take place where there are: - **(a)** Contractual clauses between the controller (*you*) or processor and the controller, processor or the recipient of the personal data in the third country or international organisation? **(b)** Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights?					
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
9.8	45	101-107	Where relying on an Adequacy Decision by the Commission, do you regularly check notices and publications for withdrawals/changes of decisions?					
9.9	46, 47	108,	Do you ensure that where you are transferring pursuant to					

		109, 110	appropriate safeguards being in place, as referred to in 9.6; that one or more of the below is used? • A legally binding and enforceable instrument between public authorities or bodies • Binding corporate rules • Standard data protection clauses adopted by the Commission • Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission • An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights • An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights					
9.10	47	110	***Where you rely on binding corporate rules to data transfers outside of the EU, do you ensure that they are: -*** • Legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees? • Expressly confer enforceable rights on data subjects with regards to the processing of their personal data?					

10. TRAINING & COMPETENCY								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
10.1			Do you educate all employees & management about the GDPR requirements and principles & the possible impact of non-compliance?					
10.2			Do you have an effective data protection training program in place?					
10.3			***Does your data protection training program cover: -*** • GDPR scope & principles? • Measures & controls for protecting data & minimising risks? • Data Protection Officer duties? • Supervisory Authority role and scope? • Codes of Conduct and/or Certifications? • Privacy Impact Assessments (PIA)? • Information Audits? • Processing Activities & Conditions? • Conditions for Consent & Privacy Notices? • Data Subject Rights & subject Access Requests? • Third Country or International Organisation Transfers • Reporting Lines & Notifications? • Privacy by Design (*i.e. data minimisation, pseudonymisation & encryption*)?					

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES	REVIEW DATE
10.4			Do you use assessment testing and/or 1:2:1 mentoring to assess and verify and evidence employee knowledge & understanding of the GDPR?					
10.5			Do you provide employees with training evaluation forms so that training is effective and adequate?					
10.6			Are staff with direct personal data processing duties provided with support, guidance and additional training regarding the GDPR requirements?					
10.7			Do employees sign confidentiality agreement and/or non-disclosure forms?					
10.8			Do you have a Training & Development Policy?					
10.9			Do employees have training records, files and annual training assessments?					
10.10			Are employees advised of their own rights under the GDPR?					
10.11			Do you have a GDPR awareness program in place for ensuring that employees understand the new Regulation prior to it coming into effect?					
11. AUDITS & MONITORING								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
11.1			Do you have documented Audit & Monitoring Policy & Procedures that have been reviewed within the past 12 months?					
11.2			Are all GDPR and associated data protection procedures audited at least annually for compliance with the Regulations and you					

			own objectives?					
11.3			Are employees monitored on an ongoing basis for compliance with the data protection laws *(i.e. email checks, account audits, monitoring phone calls etc)*					
11.4		84	Are all new processes and/or systems assessed for risks to data protection?					
11.5			Are processing activities reviewed regularly to ensure they are still valid and effective?					
11.6			Do you have mechanisms in place to spot check processing activities and staff tasks (*relating to data protection*) to ensure their compliance with your obligations and the GDPR?					
12. BREACH MANAGEMENT								
NO	**ARTICLE**	**RECITAL**	**REQUIREMENT**	**YES**	**NO**	**N/A**	**AUDITORS NOTES**	**REVIEW DATE**
12.1	34	86, 87, 88	Do you have documented data breach procedures?					
12.2			Are all staff made aware of the reporting lines for breaches?					
12.3	34	86, 87, 88	Do you maintain a data breach register and record all breaches, regardless of severity or impact?					
12.4			Is the breach register reviewed by the DPO monthly to look for patterns or duplicated issues?					

NO	ARTICLE	RECITAL	REQUIREMENT	YES	NO	N/A	AUDITORS NOTES	REVIEW DATE
12.5	34	86, 87, 88	Are all breaches investigated and corrective actions taken, regardless of the size or scope?					
12.6	34	86, 87, 88	Where a data breach has been assessed by the DPO and deemed likely to result in a risk to the rights and freedoms, do you report the breach to the Supervisory Authority within 72 hours?					
12.7	34	86, 87, 88	***Where notifying the Supervisory Authority, does the report include: -*** • A description of the nature of the personal data breach? • The categories and approximate number of data subjects concerned? • The categories and approximate number of personal data records concerned? • The name and contact details of the Data Protection Officer (or other POC where more information can be obtained)? • Description of the likely consequences of the personal data breach? • Description of the measures taken/proposed to address the personal data breach? • Measures to mitigate any possible adverse effects?					
12.8	34	86, 87, 88	Are high risk breaches reported to the data subject and the above points covered in a clear & easy to read format?					
12.9	28, 34	86, 87, 88	Where you use external processor(s), do you ensure that agreements have provisions for meeting the 72-hour					

			notification deadline if there is a breach?					

TO BE COMPLETED BY THE AUDITOR

Have all questions been completed? YES/NO **Print Name:** _____

Have all next review/action dates been set? YES/NO **Signed:** _____

1 GDPR AUDIT CHECKLIST

GENERAL DATA PROTECTION REGULATION (GDPR) IMPLEMENTATION ACTION PLAN						
CHECKLIST NO.	**SUMMARY**	**CORRECTIVE ACTION OR MITIGATING CONTROL**	**RESPONSIBLE PERSON**	**STATUS**	**DUE DATE**	**COMPLETED (√)**

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**	Yes	
	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	

	Title of document being reviewed:	Yes/No	Comments
	Have the key documents been critically appraised?	Yes	
	Are key documents cited within the policy?	Yes	
	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**	Yes	
	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**		
	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	Yes	

	Title of document being reviewed:	Yes/No	Comments
	documentation?		

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 Committee/s	IGSG/Policies and Procedures Group and Trust Executive Committee

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: **General Data Protection Regulations (GDPR) 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	*Sharon Thomas*	**Date completed**	*May 2018*
Name of responsible Director	*Daren Fradgley*		
Signature