WTC Data Protection Policy

DOCUMENT CONTROL INFORMATION			
Document type	POL (Policy)	**Full Document Number**	WTCPOL002
Version:	3.0	**Superseded Version:**	2.0
Originator:	Sheila Donegan	**Job title:**	Business Administrator
Department / Function:	Well Travelled Clinics	**Subject category:**	Information Governance
Authorship date:	16-05-2018	**Published date:**	25.05.2021
Date for Review:	30-04-2022		

Target Audience	
People who need a detailed knowledge of the document	All colleagues involved in processing personal data
People who need to know that the policy exists and have a broad understanding	All colleagues, patients and companies who use our services

Annex of Modifications		
Version	**Date of issue**	**Details of modification from previous version**

1 Introduction and Context

1.1 This policy is in line with Liverpool School of Tropical Medicine (LSTM) data protection policy. The way in which Well Travelled Clinics (WTC) processes personal data is fundamental to the trust of data subjects in the company. This includes information relating to its colleagues, patients and other individuals. We need to process 'personal data' for a variety of reasons, such as to recruit and pay colleagues, and to comply with statutory obligations (for example, health & safety requirements).

1.2 The legislative framework for this has been the Data Protection Act 1998 "the Act", however, from 25 May 2018 this has been replaced by the EU General Data Protection Regulation (GDPR) "the Regulation". The UK Parliament is also preparing a Data Protection Act (currently "Bill") to amend the GDPR for the UK, post-Brexit. This policy outlines the responsibilities of colleagues and other parties connected with in ensuring compliance with this regulation.

1.3 WTC acknowledges its obligations under the regulation and is committed to protecting the rights and freedoms of all individuals whose personal data is processed as part of its business processes.

1.4 Please read this document very carefully as it will make you aware of your responsibilities under the applicable legislation. If you fail to comply with the requirements of these policies, it may amount to misconduct, which is a disciplinary matter, and could ultimately lead to your dismissal. You should be aware that breach of data protection laws may expose WTC to enforcement action by the Information Commissioner and other regulators. Furthermore, certain breaches can give rise to personal criminal liability for you or WTC. At the very least, a breach of the legislation could damage our reputation and affect our ability to use Personal data, which would have serious consequences for WTC business.

1.5 If you have any questions about issues raised in this policy or in relation to any aspect of WTC's compliance with data protection laws then please contact the Business Administrator.

1.6 This document has been reviewed in May 2021, as per the GDPR requirements. To comply with the legislation, you must:

- Begin by complying with the data protection principles that are contained in the legislation. These are described in more detail in the subsequent sections. Make sure that you do not obtain or disclose personal data without clear authority from WTC to do so.
- The obligation not to disclose personal data, without clear authority from WTC, applies even if requests are received from the police, the Inland Revenue or any other authorised body. There are only limited circumstances in which we can disclose personal data to these organisations and each request must be considered carefully. Please check with the Business Administrator before making any disclosure.

2 Scope

2.1 This policy and the EU General Data Protection Regulation apply to all Personal data processing functions, including those performed on Personal data of the patients, employees, suppliers and partners and any other Personal data the company processes from any source handled by WTC, both that held in paper files and data held electronically. So long as the processing of the data is carried out for WTC's business purposes, it also applies regardless of where data is held, (for example, it covers data held in the clinic's and on mobile devices such as on electronic notebooks or laptops) regardless of who owns the PC/device on which it is stored.

2.2 Definitions are more widely explained at the end of this document, but "processing" data is widely defined and includes every plausible form of action that could be taken in relation to the data such as obtaining. adapting, altering, retrieving or using it in any way; sharing or disclosing it; erasing and destroying it.

2.3 This policy applies to all of WTC, including, colleagues and any outsources suppliers and contractors. Any breach of the GDPR or this policy will be dealt with under WTC's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.4 Partners and any third parties working with or for WTC, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by WTC without having first entered into a data confidentiality agreement, which imposes on the third party, obligations no less onerous than those to which WTC is committed, and which gives WTC the right to audit compliance with the agreement.

3 Roles and Responsibilities

3.1 The LSTM Board and the WTC Board of Directors are ultimately responsible for our compliance with GDPR with day-to-day responsibility delegated to the LSTM Data Protection Officer.

WTC are committed to compliance with all relevant EU and Member State laws in respect of Personal data, and protection of the "rights and freedoms" of individuals whose information WTC collects and processes in accordance with the current data protection legislation in UK, including GDPR.

Within WTC, the Managing Director is responsible for oversight of information governance including data protection matters which includes reviewing and approving policies and related guidelines. Those in managerial or supervisory roles throughout WTC are responsible for developing and encouraging good information handling practices within WTC. Day-to-day responsibility within WTC is delegated to the Business Administrator.

3.2 The Business Administrator has the following responsibilities:

- To inform and advise WTC management and colleagues about their obligations under the Regulation;
- To monitor compliance with the Regulation, the WTC data protection policies and associated framework;
- To provide advice where requested regards the data protection impact assessment and monitor its performance;
- To cooperate with the Information Commissioner's Office (ICO);
- To act as the contact point for the ICO on issues relating to processing, including "prior consultation" as outlined in Article 36 of the Regulation;
- To act as the contact point in respect of procedures such as the subject access request procedure and is the first point of call for colleagues seeking clarification on any aspect of data protection compliance.
- To be responsible for reviewing the record of processing activities annually in the light of any changes to WTC's activities and to any additional requirements identified by reviewing business processes. This record needs to be made available to the supervisory authorities when requested or required.

3.3 Colleagues with responsibilities for processing personal data will adhere to the Policy and any other guidance or procedures accompanying it.

3.4 Compliance with data protection legislation is the responsibility of all WTC who process personal data. All colleagues will undertake training and be aware of the Policy's existence.

3.5 Colleagues of WTC are responsible for ensuring that any personal data about them and supplied by them to WTC is accurate and up-to-date.

4 General Data Protection Regulation (GDPR) principles

4.1 WTC colleagues should be aware of the principles of the Regulation and ensure that these are addressed when dealing with personal data.

4.2 The first principle is **legality, transparency and fairness**:

For processing to meet the first principle you need to identify a lawful basis. This can include consent, but where this is the case the individual may have greater rights as a result, e.g. to have their data deleted. WTC will always identify that legal basis and communicate this to a data subject before processing their data. Apart from consent, other possible legal bases are:

- necessary for performance of a contract;
- compliance with a legal obligation;
- to protect the vital interests of the data subject or another person;
- for the purposes of legitimate interests or in the exercise of official authority invested in the data controller.

For special categories of data, explicit consent is usually required.

4.3 The second principle is **purpose limitation**:

- Personal data should only be 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 not be considered to be incompatible with the initial purposes.

4.4 The third principle is **minimisation**:

- WTC must not collect information that is strictly not necessary for the purpose of which it is obtained. All WTC staff are advised not to start collecting any Personal data which they are not already authorised to collect, even if they think this may assist WTC. They should check with the Business Administrator before collecting any additional Personal data.
- All data collection forms, electronic or paper-based, must include a privacy notice or a link to relevant privacy statement approved by the Managing Director.
- The Business Administrator will review all data collection methods on an annual basis to ensure that collected data continues to be adequate, relevant and not excessive.

4.5 The fourth principle is **accuracy**:

- Processing of personal data should be 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. WTC must review and update the stored data to ensure accuracy and relevance of the data. All WTC staff should attempt to avoid using guess work to decipher any documents which they cannot read clearly as this could result in WTC holding inaccurate information.
- It is the responsibility of the Data Subject to ensure that data held by WTC is accurate and up to date. Completion of a registration or application form by a Data Subject will include a statement that the data contained therein is accurate at the date of completion.
- All staff, patients and any third parties should notify WTC of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of WTC to ensure that any notification regarding change of circumstances is recorded and acted upon.
- Appropriate arrangements must be made, where third-party organisations may have been passed inaccurate or out-of-date Personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to make decisions about the individuals concerned; and for passing any correction to the Personal data to the third party where this is required.
- All rectification requests received from data subjects must be reported to the Business Administrator and responded to within one month.

4.5 The fifth principle is **storage limitation**:

- Personal data should be 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 in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific

or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- The Business Administrator is responsible to define retention periods for the data. When Personal data is retained beyond the retention period, it must be minimised/pseudonymised/encrypted to protect the identity of the Data Subject. The Business Administrator must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 The sixth principle is **integrity and confidentiality**:

- Personal data should be 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.
- In determining appropriateness of the security measures, WTC's IT team should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or patients) if a security breach occurs, the effect of any security breach on WTC itself, and any likely reputational damage including the possible loss of customer trust.
- Failure to comply with WTC's policies may lead to disciplinary action.

4.7 The seventh principle is **accountability**:

- Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." This is sometimes referred to as the "Seventh principle". WTC will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, breach notification procedures and incident response plans.

4.8 In addition, the Regulation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

5 Rights under the General Data Protection Regulation (GDPR)

5.1 Under the Regulation, a data subject has certain rights.

5.2 The first of these is the right to be informed:

- It is necessary to inform the data subject via a "privacy notice". The information given must be concise, transparent, understandable and easily accessible; communicated in clear and plain language and free of charge.

5.3 Right of access:

- Under the Regulation, individuals will have the right to obtain: confirmation that their data is being processed; access to their personal data and some supplementary information such as that which should be provided in a privacy notice. This is usually known as a "subject access request". Further information is provided in "The Subject Access Request Procedures".
- If you receive anything that looks like a subject access request, either by letter, telephone, face-to-face interview, fax, email, etc. you must pass this request immediately to the Business Administrator. WTC is under a very strict time limit of 20 working days to respond to this request and any wasted time may harm WTC.

5.4 Right to rectification:

- Data subjects are entitled to have their personal data corrected if it is inaccurate or incomplete. Self-service updating is preferred, but if this is not possible, then they should promptly action any requests for changes.

5.5 Right to erasure (right to be forgotten)

- Individuals have a right to have their personal data erased and to prevent processing in some specific situations. If a Data Subject requests to erase their personal information, please pass the request to the Business Administrator immediately.

5.6 Right to restrict processing

- In certain situations, the data subject has a right to restrict processing. A Data Subject can request to restrict processing of their data if they contest the accuracy or lawfulness of the processing and/or when they require data for defending or exercising a legal claim. If you receive anything that looks like a request to restrict processing, you must pass this to the Business Administrator immediately.

5.7 Right to data portability

- This is a new concept which did not exist in the UK's 1998 Data Protection Act and allows individuals to acquire and reuse their personal data for their own purposes, but only in certain circumstances.

5.8 Right to object

- Data subjects have the right to withdraw their consent. There are certain conditions around the right to object when the processing is being carried out for research purposes. If you receive anything that looks like a request to prevent such processing, pass it to the Business Administrator immediately. Once again, WTC is under very strict time limits for dealing with such requests.

5.9 Right in relation to automated decision making and profiling

- The data subject has a right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects them. WTC does not use automated decision making. If you receive anything that looks like an objection to an automated decision, you must pass this to the Business Administrator immediately.

5.10 Right to compensation

- Any person who has suffered material or non-material damage due to an infringement of GDPR have the right to receive compensation from WTC for the damage suffered. If you receive such a claim you should pass it to the Business Administrator immediately.

5.11 Right to lodge a complaint

- Data Subjects have the right to lodge a complaint to the Information Commissioner's Office (ICO). if they believe that WTC has breached their Data Subject rights or is non-compliant with any of the data protection provisions. If you receive such a complaint you should pass it to the Business Administrator immediately.

6. Data security and data breaches

6.1 The sixth principle "integrity and confidentiality" stipulates that personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All colleagues are therefore responsible for compliance with this principle and must follow appropriate guidance and standard operating procedures as laid down by the Business Administrator and IT Services. This applies to all personal data held in hard copy or electronic format and from wherever in the world, colleagues are operating. Examples of associated policies and guidance can be found in the list of further information at the end of this policy and include:

- "Acceptable Use of Computer and IT Facilities"
- "Information Classification Matrix"
- "Privacy Policy"
- "Crosscare Patient Administration"

6.2 When assessing appropriate technical measures, IT Services will consider the following:

- nature of the data to be protected
- risk assessment of the data
- harm that might result from a Data Loss Event
- state of technological development
- cost of implementing any measures.

6.3 When assessing appropriate organisational measures, WTC will consider the following:

- appropriate training levels throughout WTC
- measures that consider the reliability of employees (such as references Disclosure & Barring Service (DBS) Checks etc.)
- inclusion of data protection in employment contracts
- identification of disciplinary action measures for data breaches
- monitoring of staff for compliance with relevant security standards
- physical access controls to electronic and paper based records

- Adoption of a clear desk policy
- Storing of paper based data in lockable fire-proof cabinets
- Restricting the use of portable electronic devices outside of the workplace
- Restricting the use of employee's own personal devices being used in the workplace
- Adopting clear rules about passwords
- Making regular backups of Personal data on the patient administration system (Crosscare) and storing the media off-site as per Crosscare policy
- Patient registration form updated to provide email consent
- Policy updates to conform with current or soon to be implemented Data Protection Regulations i.e. the Privacy Policy.

6.4 Please note that this guidance may change as systems are enhanced or developed or as further advice is obtained from the ICO. It is important that you embed "privacy by design" principles into any current or planned project, so you should ensure that you are using the most up-to-date guidance available and check with IT Services or the Business Administrator if you are unsure.

6.5 One major change to data protection brought in by the Regulation is the reporting of data breaches. A personal data breach should be reported to the supervisory authority "…*without undue delay and, where feasible, not later than 62 hours after having become aware of it*…". The only exception to this is where the personal data breach is "…*unlikely to result in a risk to the rights and freedoms of natural persons*". WTC will put in place suitable procedures to enable this requirement to be met, but it is incumbent on all colleagues to understand this principle and to follow the procedure in the event of their identifying a potential data breach. See the "Procedure for Notification of Security Breaches" for further information.

7 Prohibited activities

7.1 The following activities are strictly prohibited:

- Using data obtained for one purpose for another supplemental purpose
- WTC must ensure that Personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All employees/staff should exercise caution when asked to disclose Personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of WTC's business.
- All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Managing Director
- Carriage of personal data on non-WTC laptops or other devices which are not encrypted to standards set by IT Services.

7.2 If you have doubts about an activity not listed above, then please seek advice from the Business Administrator.

8 Subject access requests

8.1 Under the GDPR, the data subject has the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information (this mirrors the information provided in the privacy notice i.e. purpose of processing, categories of data being processed etc.)

8.2 This right of access was previously referred to as a "subject access request" under the Data Protection Act 1888. The GDPR has brought some changes to this, most notably that the response time is reduced from forty days to one month and that no fee may be charged. Such a request for access must be handled according to the "Subject access procedures" which accompany this policy.

8.3 Third party access – this could be a party acting on behalf of the data subject. This may be allowed, but the appropriate procedures must be followed in ascertaining the right of the third party to make the request.

8.4 Freedom of Information (FOI) requests for the requester's personal data. Any FOI request which is received by WTC relating to the requester's personal data should be treated as a SAR.

8.5 When a SAR involves 3rd party information you need to seek the other individuals' consent.

8.6 Exemptions may be allowed to SARs in certain circumstances which include the prevention of crime and assessment of taxes (see below). These exemptions apply where the release of the information is "likely to prejudice" the function of the organisation to which the request is made. The advice given by the ICO is that this must constitute a "substantial chance" and not a mere risk that complying with the SAR would noticeably damage the discharge of the function concerned.

8.7 Individuals have the right to apply for a copy of any Personal data, which WTC holds about them – also called subject access request. If you receive anything that looks like a subject access request, either by letter, telephone, face-to-face interview, fax, email, etc. you must pass this request immediately to the Business Administrator. WTC is under a very strict time limit to respond to this request and any wasted time may harm the company.

All subject access requests must be processed in line with the subject access request procedure issued by the Business Administrator.

9 Release for crime and taxation

9.1 The legislation includes exemptions for the following purposes:

- The prevention or detection of crime
- The capture or prosecution of offenders
- The assessment or collection of tax or duty.

9.2 However, the exemption applies, only to the extent that complying with a SAR would be likely to prejudice the crime and taxation purposes set out above.

A set of procedures exist which must be invoked in the event of an approach by an enforcement agency (e.g. Police, UK Border Force). The member of colleagues receiving the request must immediately invoke these procedures and the release of information can only be authorised by the senior members of WTC colleagues named therein

10 Research data

10.1 WTC colleagues or students embarking on research which involves personal data should ensure that they have understood this policy and associated guidance and have documented (as per privacy by design guidance) how they will comply. Personal data obtained or used for research should be limited to the minimum amount which is reasonably required to achieve the designed academic objectives. Anonymisation techniques should be applied where possible so that the data subjects cannot be identified.

10.2 There are some exemptions in the legislation regarding data obtained for "…archiving, research and statistical purposes", for example, allowing personal data to be held for longer than the original purpose it was obtained.

11 International transfers

11.1 Personal data can only be transferred outside the European Union in compliance with the conditions for transfer set out in Chapter V of the Regulation. The "Guidance Note for the International Transfers of Personal data" outlines how transfers can be made in accordance with the Regulation.

11.2 WTC undertakes to only transfer personal data where the organisation receiving the personal data has provided adequate safeguards. These include legally binding agreements between public authorities or bodies; binding corporate rules and standard data protection clauses. Further detail is available in: "Guidance Note for International Transfers of Personal data".

11.3 International transfers are defined as moving data outside of the EU. WTC colleagues must ensure that the method of transfer they use complies with the Regulation. Any breach of the Regulation would automatically result in a higher tier fine. WTC will transfer data outside EEA only when there is an adequacy decision from the EU Commission as detailed in Article 45 or where there are appropriate safeguards, specified in Article 46 of the GDPR, in place. All data transfers outside EEA must be authorised by the Managing Director.

12 Risks and implications of breaching this policy

12.1 A serious contravention of data protection legislation which breaches the rights of a data subject can lead to fines of up to Euros 20 million (or 4% of annual global turnover) whichever is the greater and possible litigation against the individual or individuals responsible for the breach. Apart from the fine, such a contravention would be seriously damage to WTC's reputation which, in turn, could have negative impact on relationships with our funders and regulatory authorities. As a result, WTC takes its responsibilities very seriously and expects its colleagues and students to comply with this policy, and the training and guidance which has been provided.

12.2 Breaches of this policy by colleagues will be investigated, and where appropriate, formal disciplinary action may be taken up to, and including dismissal.

13 Our website

13.1 Personal information

The following principles apply to the personally identifying information we ask for and that a person provides. 'Personally, identifying information' is information that uniquely identifies the person, such as the name, physical address or email address. Any information a person supplies, including, where relevant, sensitive personal data relating to them will not be shared with 3rd parties or organisations. We would only disclose personally identifiable information to the relevant authorities if we are required to do so by law

Our website collects and uses personal information for the following reasons:

13.2 Well Travelled Clinics contact form

If a person chooses to complete and submit our contact form and provide personally identifying information (typically the name and email address), this data is stored on our site, which is hosted on a secure server, with an SSL certificate.
People can also request access, updates, deletion or more information about the data held about them at any time by emailing tropshop@LSTmed.ac.uk

13.3 Site visits tracking

Like most websites, our site uses Google Analytics to track user interaction. We use this data to determine the number of people using our site, to better understand how they find and use our web pages and to see their journey through the website.

Although Google Analytics records data such as the user geographical location, device, internet browser and operating system, none of this information personally identifies the user to us. Google Analytics also records the user computer's IP address which could be used to personally identify the user but Google do not grant us access to this. We consider Google to be a third-party data processor.

Google Analytics makes use of cookies, details of which can be found on Google's developer guides.

13.4 Email links

Should a person choose to contact us using an email link, none of the data that they supply will be stored by our website. Instead the data will be collated into an email and sent to us.

13.5 About our website's server

The WTC website is hosted by Linode within a UK data centre run by Telecity. Telecity implements high-end physical security in their data centres: All facilities are well protected by 24×7 human security, biometrics, secure monitored single person entry and video surveillance (source: Telecity). All traffic (transferral of files) between this website and the user web browser is encrypted and delivered over HTTPS.

13.6 Third party data processors

We use a number of third parties to process personal data on user behalf. These third parties have been carefully chosen and, to the best of our belief and understanding, all of them comply with current legislation. Both third parties are based in the USA and are EU-U.S. Privacy Shield compliant.
Google (Privacy policy)
Mailchimp (Privacy policy)

Our site may, from time to time, contain links to and from the websites of our partner networks and affiliates. If the user follows a link to any of these websites, they should note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before submitting any personal data to these websites.

13.7 Data breaches

We will report any unlawful data breach of our website's database or the database(s) of any of our third-party data processors to any and all relevant persons and authorities within 72 hours of the breach if it is apparent that personal data stored in an identifiable manner has been stolen.

13.8 Data controller

The data controller for our website is
Manta Ray Media Ltd
Telephone: +44 (0)20 3815 7155
Email: hello@mantaraymedia.co.uk

14 Related documents and further information

14.1 Related documents including policies, guidance and procedures are listed here:

- “Acceptable Use of Computer & IT Facilities”
- “Guidance Note for International Transfers of Personal data”
- “Information Classification Matrix”
- “Procedure for Notification of Security Breaches”.
- “Procedure for the Release of Information to Prevent or Detect Crime”
- “Subject Access Request Procedures”
- “Disciplinary procedure”
- “Privacy Policy”
- “Registration form consent”
- “Crosscare Patient Administration System”

15 Definitions

Term	Definition
Biometric data	One of the special categories of data under the Regulation, defined as 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 finger print data
Child	The GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law – as proposed in UK by the Data Protection Bill. The processing of Personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.
Consent	‘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.
Data controller	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	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data Protection Impact Assessment	A process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).
Data Protection Officer	To be appointed by a data controller where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
Data subject	An individual who is the subject of personal data. WTC processes personal data about our employees, patients, business contacts, suppliers and patients of the NHS. This data may be processed by computer, held in telephone recordings or may be held in manual filing systems. The test as to whether the manual files are covered by the Act is whether the manual files are internally and externally structured so that the user can find specific information about a particular individual easily. If the user manual files are covered by the Act, it will affect what the user can do with the Personal data contained within them.
Filing system	Any structured set of Personal data (both electronic and paper format), which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Genetic data	One of the special categories of data in the Regulation, defined as 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.
Natural person	A human being as distinguished from a person (as a corporation) created by operation of law
Personal data (also known as personally identifiable information)	Any information relating to an identified or identifiable natural person ('data subject'); Personal data means information which relates to a living and identifiable natural individual, directly or indirectly, such as names, addresses, identification numbers, account numbers, online identifier, and location data. Images caught on CCTV cameras, recorded telephone conversations 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 are also Personal data.
Personal data breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; There is an obligation on the Data Controller to report Personal data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal data or privacy of the Data Subject.

Privacy by design	The promotion of privacy and data protection compliance from the start of, and integral to all projects which involve personal data.
Processing	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.
Profiling	Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
Special categories (formerly known as sensitive personal data)	Article 9 of the GDPR refers to special categories of data, e.g.: • Racial or ethnic origin • Political opinion / affiliation • Religious or political beliefs • Trade Union membership • Genetic/biometric data (for the purpose of uniquely identifying a natural person) • Health related • Sex-life/sexual orientation To process special categories of data, in addition to lawful basis, an additional condition for processing this data must be satisfied (as detailed in Article 9 of the GDPR).
Supervising authority	An independent public authority which is established by a Member State pursuant to Article 51. In the UK, this is the Information Commissioner's Office.
Third country	Any country **other than** a member of the European Economic Area (EEA) i.e. EU Member States together with Iceland, Liechtenstein and Norway.
Third party	A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor who, under the direct authority of the controller or processor, are authorised to process Personal data.