Data Protection – GDPR

Policies and Procedures Manual

**TURNERS OCCUPATIONAL HEALTH & WELLBEING SERVICES**

Table of Contents

**POLICIES**

**TABLE OF CONTENTS**

Table of Contents

[POLICIES 3](#_Toc18650543)

[Personal Data Protection Policy 3](file:///C%3A/Users/User/Documents/Tracy%20Turner%20Ltd/Data%20Protection%20Manual%20TTLtd%20v1.0.docx#_Toc18650544)

[Personal Data Retention AND ERASURE Policy 23](file:///C%3A/Users/User/Documents/Tracy%20Turner%20Ltd/Data%20Protection%20Manual%20TTLtd%20v1.0.docx#_Toc18650545)

[IT Security Policy 32](file:///C%3A/Users/User/Documents/Tracy%20Turner%20Ltd/Data%20Protection%20Manual%20TTLtd%20v1.0.docx#_Toc18650546)

[PROCESSES & PROCEDURES 52](#_Toc18650547)

[Data Subject Rights Process 52](file:///C%3A/Users/User/Documents/Tracy%20Turner%20Ltd/Data%20Protection%20Manual%20TTLtd%20v1.0.docx#_Toc18650548)

[Personal Data Breach Process 66](file:///C%3A/Users/User/Documents/Tracy%20Turner%20Ltd/Data%20Protection%20Manual%20TTLtd%20v1.0.docx#_Toc18650550)

[NOTIFICATIONS 71](#_Toc18650551)

[REGISTERS & LOGS 84](#_Toc18650558)

# POLICIES

Personal Data Protection Policy

1. **Introduction**

This policy governs the use of personal information within Turners Occupational Health & Wellbeing Services Ltd so that all of our team members, individual contractors and other workers (Personnel) will have a clear idea of the limits of use of personal information, and where to go for further advice.

* 1. Purpose

This policy lays down the principles for the processing of personal information, whether it relates to team members, suppliers, guests, customers or others. Personal information means any information relating to a living, natural person, who can be identified either directly or indirectly. Processing personal information includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.

It is not designed to replace practical advice from either the Data Manager or the Data Protection Officer. Nor is it intended to provide all the answers to questions concerning the use of personal information in particular areas, such as ethical duties prescribed by professional bodies such as the General Medical Council or the Nursing and Midwifery Council as they would apply to occupational health practitioners, HR, IT or marketing.

Additional Guidance notes on specific issues (e.g. Subject Access Rights) are also available from Priviness Limited.

* 1. Summary

Turners Occupational Health & Wellbeing Services will use the personal information of individuals fairly, lawfully, transparently and in a manner consistent with its valid business interests and at the same time, respecting the fair and lawful privacy requirements of those individuals concerned.

* 1. Status of this policy

This policy has been approved by the Director(s) of Turners Occupational Health & Wellbeing Services. Personnel who process personal information on behalf of Turners Occupational Health & Wellbeing Services must adhere to the terms of this policy and any breach will be taken seriously and may result in formal disciplinary action.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Manager.

Any Personnel who consider this policy has not been followed should raise this matter with the Data Manager.

* 1. Further advice

Further advice may be obtained from the:

* Data Manager at info@turnersoccupationalhealth.co.uk
1. **Governing Principles**
	1. Principles

Personal information will be used within Turners Occupational Health & Wellbeing Services by its Personnel according to the principles of applicable data protection legislation (the "**DP Legislation**"), meaning the General Data Protection Regulation (“GDPR”), the Data Protection Act (“DPA”) and the Privacy and Electronic Communications Regulations ("PECR"). The principles require that personal information will have:

|  |  |
| --- | --- |
| 1. **Lawfulness, fairness & transparency**
 | The DP Legislation seeks to ensure that processing is carried out lawfully, fairly and transparently without adversely affecting the freedoms, interests and rights of the individual concerned. For personal information to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the individual, for compliance with a legal obligation, the vital interest of the data subject, or the legitimate interest of Turners Occupational Health & Wellbeing Services or the party to whom the information is disclosed.DP Legislation imposes specific requirements in relation to electronic marketing (e.g. email, Apps, social media and SMS), telephone marketing and the use of tracking or profile analysis technology (e.g. to deliver targeted online advertising). It is very important that you seek advice from internal teams, including the Data Manager before undertaking such activities on behalf of Turners Occupational Health & Wellbeing Services .Before personal information is passed to third parties, including law enforcement agencies, government bodies, investigators or anyone else, it is important that full consideration is made of the possible data protection implications of doing so. Again, please contact the Data Manager if you have any questions or are in any doubt regarding a particular request. |
| 1. **Purpose limitation**
 | Personal information may only be processed for the specific purposes notified to the individual when the information was first collected or for any other purposes specifically permitted by the DP Legislation. This means that personal information must not be collected for one purpose and then used for another, unless the other purpose is also specified.  |
| 1. **Data minimisation**
 | Only personal information that is necessary for the purposes specified should be collected. Any data which is not necessary for that purpose should not be collected in the first place. |
| 1. **Accuracy**
 | Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information should be securely destroyed. |
| 1. **Storage limitation**
 | Personal information should not be kept longer than is necessary for the purpose for which it was collected. This means that data should be destroyed or erased from our systems when it is no longer required.  |
| 1. **Integrity and confidentiality**
 | We must ensure that appropriate safeguarding measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Individual data subjects may apply to the courts for compensation if they have suffered damage or distress from such a loss. From May 2018 tough new obligations to notify, in certain situations, regulators (and affected individuals) have been introduced if the above-mentioned safeguarding measures fail to protect personal information. It is therefore very important that you immediately report any suspected incident to the Data Manager.The DP Legislation requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction, be it paper-based or in electronic format.Personal data may only be transferred to a third-party data processor (such as a supplier or service provider to Turners Occupational Health & Wellbeing Services ) if they agree to comply with those procedures and policies, or if they put in place adequate measures. DP Legislation also requires Turners Occupational Health & Wellbeing Services to have a written contract in place with all suppliers or service providers who will process their personal information. It is therefore important that procurement is involved in all such arrangements, that the correct procurement templates are used and/or that internal legal teams are consulted prior to the engagement of suppliers and partners who will either process personal information per our instructions or jointly process personal data. |
| 1. **Accountability**
 | We must ensure that we are able to evidence that we comply with DP Legislation.For example, that all the above principles have been applied, documentation is up to date, training on data protection and privacy has been completed, and security measures are complied with. |

* 1. Compliance with the principles

In order to meet the requirements of the principles Turners Occupational Health & Wellbeing Services will:

* observe the conditions regarding the fair, lawful and transparent collection and processing of personal information;
* meet its obligations to specify the purposes for which personal information is used;
* collect and process personal information only to the extent it is required for Turners Occupational Health & Wellbeing Services ’s valid business interests and where there is a legal basis for doing so;
* ensure the quality of the personal information used;
* adopt a data retention and disposal policy that includes the length of time personal information is held;
* ensure that the rights of individuals about whom personal information is held can be fully exercised under the respective DP Legislation;
* take appropriate technical and organisational safeguarding measures (which include strict Personnel access controls) to protect personal information including following the policy guidelines set out in the IT Security Policy and IT Acceptable Use Guide;
* ensure that any contractor, agent or other third party who processes personal information on Turners Occupational Health & Wellbeing Services ’s behalf does so under a written contract requiring that third party to:
* only process the personal information in accordance with Turners Occupational Health & Wellbeing Services ’s instructions; and
* take appropriate technical and organisational security measures to safeguard personal information; and
* ensure that personal information is not transferred outside the European Economic Area without suitable safeguards; and
* confirms destruction of all information. This should include both paper and electronic. Consideration should be given to backup media; and
* which contains additional data processing clauses which are specified in the DP Legislation.
	1. Responsibility for compliance

Turners Occupational Health & Wellbeing Services is a data controller (and may, in certain circumstances, also be a processor) responsible for complying with the DP Legislation. It is the responsibility of each member of Turners Occupational Health & Wellbeing Services to comply with this policy when using personal information relating to team members, customers or others.

The Data Manager has responsibility for this policy and its review.

1. **Legal Basis**

All processing must be lawful, which means that there must be one of the following legal grounds established before processing can take place:

* 1. Consent

When using consent, Turners Occupational Health & Wellbeing Services must be able to demonstrate that consent has been unequivocally given, not just implied. Consent cannot apply to children under 13 vis-à-vis online unless the holders of parental responsibility have provided it. Nor can consent be coerced, for example, forced consent as part of a contract. Consent is a valid legal basis for processing of special categories of personal information. Consent must be prominent in any privacy statement:

* freely given, specific, informed and unambiguous
* a clear affirmative action, signifying agreement to the processing of their personal information

When consent is given in the context of a statement which also concerns other matters, the request for consent needs to be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

When consent is provided, it must be able to be withdrawn at any time with as much ease as it was originally given. If withdrawn, the information must be erased[[1]](#footnote-1).

When carrying out any direct marketing using personal information Turners Occupational Health & Wellbeing Services will:

* only market to those individuals under the correct legal basis, such as consent, and for the specific purposes notified to the guest or customer when the personal information was collected;
* use safeguarding measures such as the Telephone Preference Service, Corporate Telephone Preference Service, Mailing Preference Service, Corporate Mailing Preference Service and other third-party suppression lists where appropriate;
* use standard Turners Occupational Health & Wellbeing Services consent wording; and
* require our third-party partners to use an approach compatible with this document when capturing consents on our behalf.

Any use of personal information for direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the Data Manager.

**NB** you must use the legal basis of consent for any direct marketing to private individuals that involves electronic communications, including Apps, SMS, phone and / or email. For the purpose of direct marketing to private individuals using these channels you cannot use legitimate interests, however legitimate interest is an option when direct marketing to a contact via an organisational email.

* 1. Legitimate Interests

It is always important to demonstrate the necessity for Turners Occupational Health & Wellbeing Services to process personal information for its legitimate interests if relying on this legal basis.

When using legitimate interests, Turners Occupational Health & Wellbeing Services must be able to demonstrate that there are no over-riding risks to the individuals’ interests, rights or freedoms.

Therefore, Turners Occupational Health & Wellbeing Services ’s legitimate interests when weighed up against the risks to individuals must always be considered when conducting a data protection impact assessment (required for any new system or process – or a significant change). Similarly, the mitigating measures that are applied need to be documented.

* 1. Contract

When using contract as the legal basis, Turners Occupational Health & Wellbeing Services must be able to demonstrate that the necessity of the performance of a contract (or negotiation of a contract) with the individual, for example, employee, supplier or customer / guest[[2]](#footnote-2).

**NB** - Consent is presumed not to be freely given if it does not allow separate consent to be given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

* 1. Legal Obligation

When there is a statutory obligation, Turners Occupational Health & Wellbeing Services must be able to demonstrate for the specific purposes of processing personal information what that legal obligation is, third parties who receive the personal information under the auspices of the obligation, and any retention obligations required.

* 1. Vital Interests

When using vital interests, Turners Occupational Health & Wellbeing Services must be able to demonstrate that there is a necessity to process personal information in the vital interests of the individual concerned. For example, capturing allergy information. Vital interests are most associated with medicine. Processing an individual’s personal data to protect his or others’ vital interests may occur in a situation of public health or public safety or even public interests.

* 1. Public Interest

When using public interest, Turners Occupational Health & Wellbeing Services must be able to demonstrate that there is a need to store personal information in the interests of the public. For example, for public safety and security purposes, retaining staff information to pass to emergency services personnel given some event.

1. **REQUIREMENTS**
	1. Notices

Individuals have the right to be informed regarding the specific purposes that their personal information is being processed before processing takes place, for how long the information will be stored and processed, who it is being shared with (including internationally), and if there is automated decision-making, including profiling.

|  |
| --- |
| **Example Organisation standard wording (based on the above)** |
| < . . . illustrative purposes only . . . >Example Organisation is the controller. Our contact details are:Organisation NameAddressFor queries related to this notice please contact: john.smith@example.com<The exhibitors at this event will receive your contact details as shown on this card and may contact you directly without notifying you further as this declaration constitutes your consent.><We may retain this data for up to 1 year.>If you consent to this use of your data, we will retain a record of your consent.DECLARATION OF CONSENTI agree to my data being processed as described above. Please tick the boxSignature . . . . . . . . . . . . . . . . . . . . ..Date . . . . . . . . . . . ..You have the right to withdraw consent at any time by contacting us or our Data Manager at the email address above.You have the qualified right to request access to and port your data, rectification or erasure of the data, restriction of processing, to object to the processing.You also have a right to lodge a complaint with a Supervisory Authority, for example the Information Commissioner’s Office or <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080> |

* 1. Transfers

The DP Legislation prohibits us from transferring personal information to countries outside the European Economic Area (EEA), unless we first put in place additional safeguards.

For example, before transferring information, we may need to enter into contracts with recipients in non-EEA countries which incorporate Standard Contractual Clauses approved by the EU Commission.

Any such transfers should be notified to the Data Manager stating who the data is being shared with, and if it is subject to any automated decision-making, including profiling.

* 1. Data Protection by Design / Data Protection by Default – Approach

We must ensure that our policies reflect processes and a culture of respecting privacy. This includes ensuring that we are each accountable for the security and other safeguarding measures are adhered to, as well as collecting, processing storing, and only sharing it with those authorised and required to use it, only the personal information that is required, and only for as long as it is required for.

* 1. Data Protection Impact Assessment (DPIA)

DPIA guidance is to undertake an assessment from a risk-based perspective. Any new process or system that includes innovative technologies or processing personal information or monitoring individuals on a large scale, where there is a higher risk to rights and freedoms of individuals affected.

1. **Data subject rights**
	1. Summary of Rights

The subjects of personal information held by, or on behalf of, Turners Occupational Health & Wellbeing Services ("Data Subjects") have a wide range of rights granted to them under the DP Legislation. Whilst we can make use of personal information for specific purposes and where we can lawfully justify such use, an individual can still exercise significant control over what we do. We need to operate our business and process personal information in a way which facilitates the rights of individuals to exercise this control.

Today’s DP Legislation significantly enhances the rights available to individuals. A summary of each of the rights is set out below.

It is important that requests from individuals wishing to exercise any of the rights below are quickly identified and sent to the appropriate person for preparing a response. Personnel should not respond to such requests without first discussing the matter with the Data Manager.

* 1. Right to be informed

Individuals have the right to be informed of how their personal information is being processed.

This must be provided in a privacy notice – the notice may be in the form of:

* a privacy statement or privacy policy separate to a cookie policy (which is also required);
* an email signature, other correspondence, or information board in a public area;
* a privacy clause in an Employee Handbook; or
* a clause within the Terms and Conditions of a contract.

In general, individuals must be informed about:

* the purpose for processing their personal information,
* what information is processed, and
* for how long.

The notice should also include the contact details of Turners Occupational Health & Wellbeing Services and our Data Manager.

Within the privacy notice, individuals also have the right to be informed whether any third parties are to be recipients of their personal information.

Similarly, in the same notice, individuals have the right to be informed whether their personal information will be transferred to 3rd countries or international organisations – generally outside the European Economic Area not covered by the ‘adequacy’ regime or other safeguards, such as Binding Corporate Rules or Standard Contract Clauses.

* 1. Right of access (‘Subject Access Requests’)

Individuals have the right to request that we:

* confirm, amongst other things, whether we are holding their personal information;
* provide them with a copy of that information, and
* provide them with supporting (and detailed) explanatory materials.

We must comply with Subject Access Requests without undue delay and at the latest within one month of the request (although this can be extended in limited circumstances), and we cannot charge individuals for making a request (except in specific situations). Particular care should be taken if a request from one individual would result in personal information of another individual being disclosed. [seek advice from the Data Manager about whether such information should be redacted, or its disclosure justified]

⁎ Please contact the data manager if you receive a request for the release of personal information.

* 1. Right to rectification

Individuals have the right to require us to rectify inaccuracies in personal data held about them. In some circumstances, if personal information records are incomplete or inconsistent, individuals have the right to require us to complete the data, make it consistent, or to record a supplementary statement correcting it. Advice should be sought from the Data Manager if uncertain.

* 1. Right to erase (‘the right to be forgotten’)

Individuals have the right to have their personal information erased in certain specified situations – in essence where the continued processing of it does not comply with DP Legislation.

Where an individual makes an erasure request, we must respond without undue delay and in any event within one month (although this can be extended in limited circumstances).

There are a number of exemptions which apply to such requests, and you should not assume that you should delete personal information simply because you have received a request of this nature.

Such a request should be referred to the Data Manager as soon as it is received.

* 1. Right to restriction

This right allows individuals, in certain situations, to restrict our use of their personal information. This might result in our use of it being limited to storage only and could mean we have to move personal information to separate IT systems, or temporarily block access to it.

This issue could arise in a situation where an individual is disputing the accuracy of information we hold, or where they are objecting to our right to continue to use their information and we need to take some time to establish whether we have a right to continue to do so.

Such a request should be referred to the Data manager as soon as it is received. And advice should be sought from the Data Manager if uncertain.

* 1. Right to data portability

Data portability goes beyond rights of access and requires us to provide, on request, information to individuals in a structured, commonly used and machine-readable format. We could also be asked by an individual to transmit personal information directly to another data controller in the same format. This right only applies to electronic records which have been provided to us by the individual themselves or generated from their activity or are our observations of their activity (but not subsequent analysis of such activity), and only where we hold the personal information because we have the individual’s consent or because we are fulfilling a contract with them.

Such a request should be referred to the Data manager as soon as it is received.

* 1. Right to object

Individuals have an absolute right to object to their personal information being processed for the purpose of direct marketing. If we receive any such objection, we must immediately cease such marketing activities in respect of that individual.

Individuals have a wider right to object to processing we undertake which is justified on the basis that it is in our legitimate interests (rather than because we have their consent). If we receive an objection of this nature, we must assess the objection and carefully consider if we can demonstrate compelling legal grounds to continue to process the personal information.

Such a request should be referred to the Data manager as soon as it is received.

* 1. Rights in relation to automated decision-making, including profiling

Individuals have rights which apply if we take decisions about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on the individuals. An example of this would be the use of an algorithm to analyse alumni data and decide which groups of people receive preferential promotional offers.

We can use such automated decision making in circumstances where we need to do so in order for us to enter into a contract with the individual, or where we have their explicit consent. However, we need to be transparent with individuals about what decisions are taken in this way, and we may need to put in place additional protective measures to protect the individuals concerned.

Such a request should be referred to the Data manager as soon as it is received.

* 1. Right to complain

Individuals have the right to bring a complaint to the Information Commissioner, or other supervisory authority. https://ico.org.uk/make-a-complaint/

* 1. Right to bring legal proceedings

Individuals have the right to seek judicial remedy through the Courts.

* 1. Requests

Team members, customers and other subjects of personal information held by, or on behalf of Turners Occupational Health & Wellbeing Services may exercise any of the rights specified above. These rights are subject to certain exemptions which are set out in the DP Legislation.

Any team member, customer or other subject of personal information wishing to exercise any of these rights should make the request in writing using the prescribed form to the Data Manager.

Turners Occupational Health & Wellbeing Services aims to comply with any requests in relation to personal information as quickly as possible and in any event within the time specified by DP Legislation.

1. **Personnel responsibilities**
	1. Responsibility for our own data.

All Personnel are responsible for:

* + - checking any personal information which they provide to Turners Occupational Health & Wellbeing Services is accurate and up to date;
		- informing Turners Occupational Health & Wellbeing Services of any changes to personal information which they have provided, for example change of address; and
		- checking any information that Turners Occupational Health & Wellbeing Services may send out from time to time, for example giving details of personal information that is held by Turners Occupational Health & Wellbeing Services .
	1. Responsibility for other’s data

If, as part of their responsibilities, Personnel have access to or use personal information about other people as part of their employment duties (for example, customer or guest personal information) they must comply with this policy and in Turners Occupational Health & Wellbeing Services ’s other policies and procedures for processing personal information.

As an individual you are responsible for ensuring that:

* Any personal data that you hold is kept securely
* Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
* Personal information is not transferred internationally without checking first that the right safeguards are in place.
* You avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be locked out of sight
* Passwords and logon information are not disclosed to anyone else
* Personal information is kept in a locked filing cabinet, or in a locked drawer, or
* If it is computerised, be password protected, or if kept temporarily on portable media be password protected and kept securely.
* If you are aware of a breach of security with passwords or logon information the Data Manager or the Data Protection Officer must be informed immediately.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. In particular any **deliberate** or **serious** breachof this Data Protection Policy by a member of staff may lead to dismissal and even to criminal prosecution.

* 1. Access Restriction

Only those Personnel who strictly require access to personal information for their role should have such access, and all Personnel must make sure that personal information is not shared with Personnel who do not need to see it.

* 1. Special Categories

Personal information about Personnel and others may include special categories of personal information or other information that needs to be treated sensitively. This is personal information relating to an individual's:

* racial or ethnic origin;
* political opinions;
* religious beliefs or other beliefs of a similar nature;
* membership of a trade union;
* physical or mental health or condition;
* sexual life;
* biometric or genetic data (e.g. facial or iris imaging, or biological sample information.)
* commission or alleged commission of an offence;
* any proceedings for any offence or alleged offence, the disposal of such proceedings or any sentence imposed by a court

Particular care must be taken when dealing with any personal information falling under one or more of these headings. If in doubt, do take advice from the Data Manager or the Data Protection Officer. In general, such personal information must be kept very secure and must only be allowed to be seen by a restricted number of people who need to know it. The Data Manager will act as an intermediary between the organisation, employees, suppliers, customers, partners and others.

1. **Email**

Due to the ease with which large quantities of personal data can be accidentally or inappropriately exposed when using email staff should be particularly careful to use email in a considered manner. In particular:

* + - Email to addresses outside the “@turneresoccupationalhealth.co.uk” domain should not include personal data beyond simple contact information (name, email, telephone, address, job title and place of work). If more extensive data needs to be provided an encrypted attachment can be used (MS Office encryption is adequate for low risk data) or a specialised secure transfer option may be used in high risk cases.
		- If using an encrypted email attachment to send personal data do not include the password in the same email and preferably use a different communication method to send the password (e.g. SMS).
		- Emails sent from “@turnersoccupationalhealth.co.uk” addresses to “@turnersoccupationalhhealth.co.uk” addresses are restricted to the secure environment and may include personal data.
		- Do not include any personal information in the “Subject” field of email regardless of the recipient, in particular do not include names or other potential identifiers.
		- Staff should make it a habit to preferentially use “Bcc” rather than “Cc”, “Cc” should only be used where it is necessary for all recipients to see replies.
		- When using Distribution Lists to send emails to those outside the organisation, ensure that email addresses are not shared. Use the “Bcc” facility so that email addresses are not displayed.
1. **Retention**
	1. Data storage

First of all, it is important to have an overview of where personal data is stored in Turners Occupational Health & Wellbeing Services . This may include:

* own servers;
* third party servers;
* email accounts;
* desktops;
* employee-owned device (BYOD);
* backup storage; and/or
* paper files.
	1. General retention periods

Generally personal data should only be retained for as long as necessary. The retention periods can differ based on the type of data processed, the purpose of processing or other factors. Issues to consider include:

* Whether any legal requirements apply for the retention of any particular data. For example;
> Trade law; > Tax law; > Employment law; > Administrative law; > Regulations regarding certain professions, e.g. medical.
* In the absence of any legal requirements, personal data may only be retained for as long as necessary, for the purpose of processing. This means data is to be deleted e.g. when;
> the data subject has withdrawn consent to processing; > a contract has been performed or cannot be performed anymore; or > the data is no longer up to date.
* Has the data subject requested the erasure of data or the restriction of processing?
* Is the retention still necessary for the original purpose of processing?
* Exceptions may apply to the processing for historical, statistical or scientific purposes.
	1. During the retention period
* Establish periodical reviews of data retained.
* Establish and verify retention periods for data considering the following categories;
> the requirements of your business; > type of personal data; > purpose of processing; > lawful grounds for processing; and > categories of data subjects.
* If precise retention periods cannot be established, identify criteria by which the period can be determined.
* Establish periodical reviews of data retained.
	1. Expiration of the retention period

After the expiration of the applicable retention period personal data does not necessarily have to be completely erased. It is sufficient to anonymise the data. This may, for example, be achieved by means of;

* erasure of the unique identifiers which allow the allocation of a data set to a unique person;
* erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
* separation of personal data from non-identifying information (e.g. an order number from the customer’s name and address); or
* aggregation of personal data in a way that no allocation to any individual is possible.

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

* the pool of data has grown so much that personal identification is not possible based on the information retained; or
* the identifying data has already been deleted.
	1. Information obligations

In addition to other information obligations, in the context of data retention data subjects must be informed of:

* the retention period;
* if no fixed retention period can be provided – the criteria used to determine that period; and
* the new retention period if the purpose of processing has changed after personal data has been obtained.
1. **Medical Information**

The organisation will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes.

We will only use the information in the protection of the health and safety of the individual.

As well as complying with the Data Protection legislation we will also comply with ethical duties prescribed by professional bodies such as the General Medical Council, the Nursing and Midwifery Council, the Health and Care Professions Council and the SEQOHS accreditation standards.

1. **Audit**

At the beginning of each financial year, Turners Occupational Health & Wellbeing Services shall undertake a data protection audit to benchmark year-on-year compliance and improvement.

Personal Data Retention AND ERASURE Policy

1. **Introduction**
	1. Information is one of the Turners Occupational Health & Wellbeing Services ’s corporate assets; in the course of carrying out its’ various functions, Turners Occupational Health & Wellbeing Services accumulates information from both individuals and external organisations. Turners Occupational Health & Wellbeing Services also generates a wide range of data, which is recorded in documents and records.
	2. These documents and records are in several different formats, examples of which include, (but are not limited to) communications such as letters, emails and attendance notes; financial information including invoices, statements and reports; medical records and licences; legal documents such as contracts and deeds; and information relating to various types of applications, including forms, plans, drawings, and photographs.
	3. For the purposes of this Policy, the terms ‘document’ and ‘records’ include information in both hard copy and electronic form.
	4. In certain circumstances it will be necessary to retain specific documents in order to fulfil statutory or regulatory requirements and also to meet operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes, and also to preserve information which has historic value.
	5. Premature destruction of documents could result in inability to defend litigious claims, operational difficulties and failure to comply with the Data Protection Act 2018.
	6. Equally, the retention of all documents and records is impractical and appropriate disposal is encouraged. Disposal will assist Turners Occupational Health & Wellbeing Services to maintain sufficient electronic and office storage space and will de-clutter office accommodation, resulting in a more desirable working environment. Lengthy or indefinite retention of personal information could result in Turners Occupational Health & Wellbeing Services breaching the Data Protection Act 2018.
	7. It is important for the above reasons that Turners Occupational Health & Wellbeing Services has in place systems for the timely and secure disposal of documents and records that are no longer required for business purposes.
2. **Aims and Objectives**
	1. The key objective of this Policy is to provide Turners Occupational Health & Wellbeing Services with a simple framework which will govern decisions on whether a particular document should be retained or disposed of. In the case of documents which are to be retained by Turners Occupational Health & Wellbeing Services the Policy includes guidance on the format in which they should be retained and appropriate retention periods.
	2. Implementation of the Policy should save staff time when retrieving information, in particular by reducing the amount of information that may be held unnecessarily.
	3. The Policy clarifies the different roles of staff in relation to document retention and disposal in order that they understand their responsibilities, and who to refer to if they are unsure about any document and require clarification.
	4. It is envisaged that this Policy will assist the Data Manager in securing compliance with legal and regulatory requirements, including the COSHH Regulations 2002, the Freedom of Information Act 2000, the Environmental Information Regulations 2005, the Data Protection Act 2018 and the Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. In addition to assisting officers in their day to day business, this should also ensure that searches for information requested under the Freedom of Information legislation are as quick as possible.
	5. Additionally, the Policy should help to ensure that Turners Occupational Health & Wellbeing Services archives, records and documents that are of historical value appropriately for the benefit of future generations.
3. **Scope**
	1. This Document Retention Policy applies to all information held by Turners Occupational Health & Wellbeing Services and its external service providers where they are processing information on Turners Occupational Health & Wellbeing Services ’s behalf.
4. **Policy Statement**
	1. The Data Manager will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its’ statutory functions and the provision of services.
5. **Retention and Disposal Policy**
	1. Decisions relating to the retention and disposal of documentation should be taken in accordance with this Policy, in particular;
* Appendix 1 – Disposal and Retention Considerations – a checklist to be followed where the disposal of any document is being considered.
* Appendix 2 – Document Retention Schedules – Comprehensive guidance on the recommended and statutory minimum retention periods for specific types of documents and records.
	1. In circumstances where a retention period of a specific document has expired, a review should always be carried out prior to a decision being made to dispose of it. This review should not be particularly time consuming and should be straightforward. If the decision to dispose of a document is taken, then consideration should be given to the method of disposal to be used.
1. **Roles and Responsibilities**
	1. The Data Manager will be responsible for determining (in accordance with this Policy) whether to retain or dispose of specific documents within the remit of their service area.
	2. The Data Manager may delegate the operational aspect of this function to one or more members of staff.
	3. The Data Manager should seek legal advice if she is uncertain as to whether minimum retention periods are prescribed by law, or whether the retention of a document is necessary to protect Turners Occupational Health & Wellbeing Services ’s position where a potential claim has been identified.
2. **Disposal**
	1. Confidential waste documents should be stored securely pending destruction in a secure storage area within Turners Occupational Health & Wellbeing Services offices. It is essential that any documents which are to be thrown away and contain confidential or personal data must be disposed of in the correct way, in order to avoid breaches of confidence or of the Data Protection Act 2018.
	2. Records of disposal should be maintained by each service area, and should detail the document disposed of, the date and who authorised the document’s disposal.

**APPENDIX 1**

**Disposal and Retention Considerations**

Each of the following questions and guidance should be considered prior to the disposal of any document.

1. **Has the document been appraised?**
* Check that the nature and contents of the document is suitable for disposal.
1. **Is retention required to fulfil statutory obligations or other regulatory obligations?**
* Specific legislation setting out mandatory retention periods for documentation should be considered
1. **Is retention required for evidence?**
* Keep any documents which may be required for legal proceedings until the threat of proceedings has passed.
* The limitation period for commencing litigation should also be a key consideration. This is governed by the Limitation Act 1980 and the main time limits that apply directly are;
* Contract or tort (such as negligence or nuisance) claims (other than personal injury) cannot be brought after six years from the date on which the cause of the action occurred.
* Personal injury claims cannot be brought after three years from the date on which the cause of action occurred.
* Claims based on provisions contained in documents that are ‘under seal’ cannot be brought after twelve years from the date on which the cause of action occurred.
1. **Is retention required to meet the operational needs of the service?**
* Consider whether the document in question may be useful for future reference, as a precedent or for performance management purposes
1. **Is retention required because the document or record is of historic interest or intrinsic value?**
* In most cases this consideration will not be relevant.
* If a particular document has historic or financial value, consideration should be given to whether it should be retained by Turners Occupational Health & Wellbeing Services or alternatively by an external body, such as the County Archivist.
* The transfer, long term retention or disposal of such documents must be authorised by the Data Manager.

**APPENDIX 2**

**Document Retention Schedules**

1. **Introduction**

The following schedules provide guidance on the retention periods applicable to a wide range of Turners Occupational Health & Wellbeing Services documents vis-à-vis personal data.

1. **Explanation of Retention Schedule Headings**
	1. Document Description – The Section defines each document.
	2. Retention Trigger – The point at which the retention period begins.
	3. Retention Period – This entry provides the guidance as to whether the document should be retained, and if so, for how long.
	4. Action – What is to be done at the end of the retention period
	5. Justification / Authority – This section provides the formal or informal reasons for retaining the record for the appropriate time period.
	6. Asset Owner – which person or job role is responsible for the document and its disposal
2. **Archiving**

The method of archiving selected for a particular document will vary between services and will depend on the type and format of documents. Staff should refer to the Data Manager for guidance on where documents should be archived if they are unsure. Archiving may include but will not be limited to electronic storage on records management systems, storage in secure filing cabinets, strong rooms or other designated areas within Turners Occupational Health & Wellbeing Services and in some limited cases sending documents to external bodies such as the Local Archives or museums.

**Appendix 3**

**Data Retention Schedule Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Document Description** | **Retention Trigger** | **Retention Period** | **Action** | **Authority/ Justification** | **Information Asset Owner** |
| **HR and Admin** |
|  | Payroll time sheets | End of Financial Year | 6 years | Destroy | HM Treasury guidelines, National Audit Office advice, Companies Act 2006, Taxes Management Act 1970 |  |
| Expense forms | End of Financial Year | 6 years | Destroy | HM Treasury guidelines, National Audit Office advice, Companies Act 2006, Taxes Management Act 1970 |  |
| Unsuccessful Recruitment Candidate Information (including third party referee details provided by the applicant) | Last Action | 6 months | Destroy | CIPD guidance, best practice |  |
| Employee contract | Termination of Employment | 5 years | Destroy | CIPD guidance, best practice |  |
| Copies of employee certifications and qualifications | Termination of Employment | 5 years | Destroy | CIPD guidance, best practice |  |
| Employee appraisal and personal development plans | Termination of Employment | 5 years | Destroy | CIPD guidance, best practice |  |
| Accident Book | Creation | 7 years | Destroy | RIDDOR 2013 |  |
| Annual leave records | Termination of Employment | 5 years | Destroy | CIPD guidance, best practice |  |
| Absence records | Termination of Employment | 5 years | Destroy | CIPD guidance, best practice |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Communications and Marketing** |
|  | Staff Mailboxes and Outlook | Creation | 12 months | Destroy | Business Need |  |
| Customer reviews | Loading onto website | 2 years | Destroy | Business Need |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **Commercial** |
|  | Invoices | End of Financial Year | 6 years | Destroy | HM Treasury guidelines, National Audit Office advice, Companies Act 2006 |  |
| Worker Health Data | Creation | 6 years after employment with client ceases or worker reaches the age of 75, whichever is sooner | Destroy | COSHH regulations 2002 |  |
| Health Surveillance Data | Creation | 50 yrears | Destroy | COSHH regulations 2002 |  |
| Worker Health Record | Creation  | 6 years | Destroy | FOM ethics guidance, COSHH regulations 2002 |  |
| Worker Medical Reports | Creation  | 6 years | Destroy | FOM ethics guidance, COSHH regulations 2002 |  |
| Drug and Alcohol test records | Creation | 1 month | Destroy | Business Need |  |
|  |  |  |  |  |  |
|  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

IT Security Policy

1. **Software Management**
	1. Introduction

This section sets out how the software which runs Turners Occupational Health & Wellbeing Services ’s IT systems and services is managed. It includes controls on the installation, maintenance and use of software, with appropriate procedures for upgrades to minimise the risk to information and information systems.

* 1. Scope
* This policy is applicable to all equipment that connects to the Turners Occupational Health & Wellbeing Services fixed and wireless network.
* This policy should be familiar to all staff involved in the specification, installation and maintenance of software.
	1. Software Security Management
* All software procurement or installation should only be undertaken with the approval of IT Services.
* There must be a nominated individual or business unit responsible for every item of software deployed on the Turners Occupational Health & Wellbeing Services network.
* Software applications are to be managed by suitably trained and qualified staff to oversee their day to day running, and to preserve security and integrity in collaboration with nominated individual application owners.
* All staff managing software applications shall be given relevant training in information security issues.
* The procurement or implementation of new or upgraded software must be carefully planned and managed in conjunction with IT Services. Any development for or by Turners Occupational Health & Wellbeing Services must document the requirements for Information Security.
* Information security risks associated with the procurement or implementation of new, or upgraded, software must use a combination of procedural and technical controls to mitigate any risks.
* All software implemented should be subject to Turners Occupational Health & Wellbeing Services ’s release management, version control, change approval and management processes.

	1. Change Control
* For all Turners Occupational Health & Wellbeing Services owned and managed equipment, formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software.
* All changes to operating systems and ancillary software must be properly authorised and must be tested appropriately before changes are moved to the live environment to ensure there is no adverse impact on Turners Occupational Health & Wellbeing Services operations or security.

	1. Software Development
* Modifications to vendor supplied software shall be avoided as far as possible, and only strictly controlled essential changes shall be permitted, after agreement with the vendor and IT Services, and the development of interfacing software shall only be undertaken in a planned and controlled manner.
* Upgrades or other changes to locally developed software must be assessed to mitigate any potential risk to information security.
	1. Software Regulation
* The use of illegal software and using software for illegal activities is not permitted and may lead to disciplinary action.
* All software installed on Turners Occupational Health & Wellbeing Services computer systems must have an appropriate licence covering its intended use.
* Use of software which tests or attempts to break Turners Occupational Health & Wellbeing Services system or network security is prohibited unless the Data Manager has been notified and has given authorisation.
* Use of software which causes operational problems, causes inconvenience to others, or which makes demands on resources which are excessive or cannot be justified, will be prohibited.
* Software found on Turners Occupational Health & Wellbeing Services IT systems and services which incorporates malware of any type is liable to be automatically or manually removed or deactivated.
* Any system that monitors the activities of other people, including for the purpose of gathering personal information is not permitted unless authorised by a Turners Occupational Health & Wellbeing Services Director.
1. **Network Management**
	1. Introduction

This section will define how Turners Occupational Health & Wellbeing Services networks are designed and IT systems, services and devices are connected to them. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of the Data Protection Policy.

* 1. Scope
* To define Turners Occupational Health & Wellbeing Services ’s policy for designing, controlling and managing Turners Occupational Health & Wellbeing Services ’s network.
* Enabling the movement of data that supports Turners Occupational Health & Wellbeing Services ’s business and disabling the movement of data that hinders Turners Occupational Health & Wellbeing Services ’s business needs over the networks for which Turners Occupational Health & Wellbeing Services is responsible.
	1. Definitions
* End User Network Device – any network enabled device which is the initial source or ultimate destination in a data network.
* Network Device – a device such as a switch or router through which data passes on its journey to or from an End User Network Device.
* Network Interface – part of a network device or end user network device that enables it to communicate via a network, there may be more than one interface on a device.
* Local Area Network (LAN) – a computer network that spans a relatively small area, such as a building.
* Network Services manager – The person appointed by Turners Occupational Health & Wellbeing Services as the person responsible for the management of Turners Occupational Health & Wellbeing Services network.
* System Owner – The manager of individual systems or services such as email or websites. Can include PC groups or LAN partitions.
	1. Management of the Network
* Turners Occupational Health & Wellbeing Services ’s network shall be managed by suitably authorised and qualified staff appointed by a Turners Occupational Health & Wellbeing Services Director(s) to oversee its day to day running and to preserve its security and integrity in collaboration with nominated individual system owners.
* Planned reconfiguration of the network will use formal, auditable change control procedures and appropriate risk management.
* Where there is a risk to the security or quality of service to the network, the Network Services manager is authorised to make emergency changes to restore service.
* The overall control of the IP address scheme is managed by the Network Services Manager, although this may be delegated to nominated system owners for limited IP address management.
* Users of the network are advised that network management procedures may include procedures such as:
	+ Probing devices to test security.
	+ Monitoring of network traffic to detect operational issues.
	+ Recording of network traffic to detect possible policy violations.
	+ Validation that data travelling across the network is legitimate and does not have virus content, is not of an offensive nature, and cannot be detrimental to performance or management of any device or end user device on the network.
	+ Monitoring, filtering and blocking of websites and other services where necessary, in order to fulfil Turners Occupational Health & Wellbeing Services ’s statutory and regulatory responsibilities
	1. Network Architecture
* The network must be designed and configured to deliver performance, reliability and security suitable for the requirements of Turners Occupational Health & Wellbeing Services .
* The network shall be segregated into separate VLANs on the basis of security requirements. These domains can have controls to prevent unauthorised access to Turners Occupational Health & Wellbeing Services ’s critical business systems, where appropriate.
* LANs in individual buildings or departments should normally be designed and installed by the network management team. In other cases, the Network Services manager reserves the right to check the installation before connecting it to Turners Occupational Health & Wellbeing Services ’s core network.
* No changes to the network infrastructure, such as the introduction of a router, switch or wireless access point, is permitted without prior approval from the Network Services manager.
* Records of all active and inactive network device locations and configurations shall be maintained.
	1. Physical Security and Integrity
* Reasonable measures based on a risk assessment, and regulatory compliance must be taken to protect rooms containing servers, active network devices and patching panels from threats such as fire, water, accidental damage, security breaches and theft.
* Physical access to rooms containing servers, active network devices and patching panels shall be restricted to:
	+ A list of authorised staff maintained by the relevant system or Network Services Manager.
	+ Other individuals providing that their entry has been approved by the relevant system or Network Services Manager.
* Any device that is running a service that conflicts with centrally managed services such as DHCP, etc. must not be connected to the network without prior agreement with the Network Services manager.
	1. Controlling Access
* Access control procedures must provide adequate safeguards through robust identification and authentication techniques.
* Only devices owned by Turners Occupational Health & Wellbeing Services or recognised partner organisations may be connected to the wired network, except under special circumstances, approved by the Network Services manager.
* Personal devices may be used on the wireless network only after registration and authentication.
* All devices connecting to Turners Occupational Health & Wellbeing Services network both wired and wireless must conform to Turners Occupational Health & Wellbeing Services policies.
* Remote administrative connection to Turners Occupational Health & Wellbeing Services network and resources will only be permitted from authorised users and devices over suitably secured connections.
1. **User Management**
	1. Introduction
* This section governs:
	+ The creation, management and de-provisioning of user accounts.
	+ The granting and revocation of authorised privileges associated with a user-account.
	+ The authentication (usually a secret password) by which the user establishes their right to use the account.
	1. Scope
* This section applies to all accounts on Turners Occupational Health & Wellbeing Services IT systems and services directly connected to networks which are managed by Turners Occupational Health & Wellbeing Services . This includes operating system (Windows, Linux, Solaris etc.), and application software accounts (HR, Accounts, Database, etc.).
* This document includes statements on:
	+ Access Control
	+ Managing Privileges
	+ Authentication/Password Management
	1. Access Control
* Manual creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.
* Automated creation of user accounts will be driven by authorised feeder systems according to criteria agreed with the service owners.
* The person enacting any change in a user account must be different from the one authorising/requesting the change.
* Logs will be kept of all account creation/deletion/changes.
* Account details will only be divulged to the user after proof of identity has been established.
	1. Managing Privileges
* A user account should have the least privilege which is sufficient for the user to perform their role within Turners Occupational Health & Wellbeing Services and access to information and information systems and services must be driven by business requirements.
* Changes in the privilege of an account must be authorised by the user’s line manager or a nominated “owner” of the information system to which the account affects.
* Users’ privilege rights will be periodically reviewed.
* Procedures shall be established to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves Turners Occupational Health & Wellbeing Services .
* User accounts should be disabled immediately once the user leaves Turners Occupational Health & Wellbeing Services or after an agreed period. The user’s data will not be deleted until after a period agreed with IT Services management and service owners.
* Users should be informed of their responsibility to inform information system owners of any change in their role which might affect their privileges. IT Services should be informed as part of the starters/leavers process.
	1. Managing Elevated Privileges
* Users whose work requires system administration access will be given a separate specialist account for this purpose, in addition to their standard user account.
* System administration accounts may use the same password policy as other accounts, but on some systems may have a separate password policy, as required by that system/service.
* In all other ways, these system administration accounts should be managed, and the user is responsible for them similarly to standard accounts.
	1. Authentication/Password Management
* All users will have a unique identifier for any Turners Occupational Health & Wellbeing Services IT system and services.
* The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.
* The account must not be used by the user where there is a possibility that the account details may be revealed.
* Passwords can only be changed by the user or suitably trained and authorised staff.
* If a user suspects their password is no longer secret it must be changed immediately, and the system “owner” notified.
1. **Wireless Communication**
	1. Introduction

This section sets out how wireless communications equipment and users connect to Turners Occupational Health & Wellbeing Services ’s networks. The policy prohibits access to Turners Occupational Health & Wellbeing Services ’s internal networks via any unsecured wireless communication mechanisms, other than those explicitly mentioned in the policy. Only wireless systems that meet the requirements of this policy and are approved by IT Services can be connected to Turners Occupational Health & Wellbeing Services ’s networks.

* 1. Scope

This section covers all wireless data communication devices (e.g. personal computers, cellular phones, smartphones, tablets, PDA’s etc.) connected to any of Turners Occupational Health & Wellbeing Services ’s internal networks. This includes any form of wireless communication device capable of transmitting data. Wireless devices and/or networks without any connectivity to Turners Occupational Health & Wellbeing Services ’s networks do not fall under the purview of this policy.

IT Services must approve exceptions to this policy in advance.

* 1. Wireless Policy Statement
* Statement of Authority
	+ Responsibility for Wireless communication resources resides with IT Services.
	+ IT Services must approve all installations of Wireless access points across all sites. Policies and guidelines for deployment of these systems are essential to prevent interference between different implementations, other uses of the wireless spectrum, and maintain a quality of service connection to a diverse user community.
	1. Turners Occupational Health & Wellbeing Services Users Access to Wireless
* Wireless access to Turners Occupational Health & Wellbeing Services network, is provided by the agreed Turners Occupational Health & Wellbeing Services supported wireless access service.
* All wireless access to Turners Occupational Health & Wellbeing Services network will be encrypted and authenticated, using approved protocols and infrastructure.
	1. Visitor Access to Wireless
* Wireless access for visitors to Turners Occupational Health & Wellbeing Services , will be available at all facilities where wireless access has been deployed.
* Wireless access for visitors is provided through an encrypted connection with a password provided on request.
* Wireless access for all visitors will be managed through a web-based authentication system.
* Wireless access for visitors is restricted to basic web access.
* Information relating to operational documentation including coverage locations, end user documentation and service information can be found at the Turners Occupational Health & Wellbeing Services offices.
	1. Wireless Request Procedure

Requests for wireless networking can be made to IT Services using the Wireless Request Procedure and any request must be made with the approval of the appropriate Manager and must outline how the request supports the business needs and aims of Turners Occupational Health & Wellbeing Services .

* 1. Definitions
* Wireless Network: the network technology that uses radio frequency to connect computing devices to a wired port on the Turners Occupational Health & Wellbeing Services network.
* Wireless infrastructure: The wireless access points, antennas, cabling, power and network hardware associated with the deployment of a wireless network.
* Access Point: A network device that serves as a common connection point for devices in a wireless network. Access points use wireless antennas instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and are usually connected to the wired network.
* Coverage: The physical area where a level of wireless connectivity is available.
1. **Use of Computers**
	1. Introduction

This section defines the acceptable actions of any individual who interacts with Turners Occupational Health & Wellbeing Services IT systems and services. The individual may be an anonymous user of public services (for example, browsing Turners Occupational Health & Wellbeing Services web pages) or they may be an authenticated user of authorised services (for example sending and receiving Turners Occupational Health & Wellbeing Services email). To be covered by this section, the individual will, either actively or passively, make decisions which in turn cause some computation to be done on Turners Occupational Health & Wellbeing Services IT systems and services.

* 1. Scope

This section applies to all users of Turners Occupational Health & Wellbeing Services IT systems and services.

Unless explicitly stated otherwise in this policy, the Acceptable Use Policy applies to all users of Turners Occupational Health & Wellbeing Services IT systems and services.

* 1. Department Policies and Regulations

Where necessary, a team member may request to implement different policies relating to the use of Turners Occupational Health & Wellbeing Services IT systems and services for which they have responsibility, subject to agreement with a Director of Turners Occupational Health & Wellbeing Services .

* 1. Acceptable Use of Turners Occupational Health & Wellbeing Services IT Facilities

Subject to clauses in section 5 below, Turners Occupational Health & Wellbeing Services IT systems and services may be used for any lawful activity which furthers the aims of Turners Occupational Health & Wellbeing Services and is consistent with the policies of Turners Occupational Health & Wellbeing Services , both at the time of use and in the reasonably foreseeable future after the time of use.

* 1. Personal use

Subject to clauses in section 5 below, authenticated individuals are allowed to make reasonable use of Turners Occupational Health & Wellbeing Services IT systems and services provided that use does not interfere with the performance of their duties, cause financial loss to Turners Occupational Health & Wellbeing Services or cause any difficulty or distress to others.

* 1. Commercial use
	+ A user must obtain explicit permission from the appropriate Manager to use Turners Occupational Health & Wellbeing Services IT systems and services for commercial gain and this may be subject to a charge
	+ Authentication (user ids and passwords): where a user has been issued with a user ID and password, the user is presumed to be responsible for all activity attributable to that identity. To that end:
	+ The user will take all reasonable steps to prevent their personal identity from being used by anyone else.
	+ Administrative account holders will also take all reasonable steps to prevent the administrative identity from being used by anyone else. In particular, passwords must be kept unpredictable to anyone except the legitimate account holder.
	+ If a user suspects that their password is no longer secret, they should change their password at the first opportunity.
	+ If you have an impairment that prevents you from entering your own username and password, you are permitted to share these details with your nominated support person.
	+ Where the user has been allocated a personal computer (such as a laptop or desktop) by Turners Occupational Health & Wellbeing Services , the user should ensure the device is shutdown at the end of the working day.
	1. Unacceptable Use of Turners Occupational Health & Wellbeing Services IT Systems and Services

The list of unacceptable uses of Turners Occupational Health & Wellbeing Services IT systems and services listed below is applicable to all Turners Occupational Health & Wellbeing Services IT systems and services and is consistent with the Acceptable Use Policy.

* Any illegal activity.
* The creation, display, download, production, store, circulation or transmission of unlawful material, or material that is indecent, offensive, defamatory, racist, threatening, discriminatory or extremist in any form or medium is strictly forbidden. Turners Occupational Health & Wellbeing Services reserves the right to block or monitor access to such material.
* Staff who requires legitimate access to the types of materials outlined in clause 5.2 must obtain an explicitly signed waiver.
* Continuing to use an item of networking software or hardware after a Director of Turners Occupational Health & Wellbeing Services has requested that use cease because it is causing disruption to the correct functioning of Turners Occupational Health & Wellbeing Services systems.
* Any attempt to bypass information security safeguards and policies embedded into Turners Occupational Health & Wellbeing Services network.
* Deliberate unauthorised access to Turners Occupational Health & Wellbeing Services IT systems and services.
* Using “open access” computing facilities (such as public or library computers) for recreational or other non-Turners Occupational Health & Wellbeing Services work when there are others waiting to use the resource.
* Authenticated sessions: a user must not leave an authenticated (i.e. logged in) session unattended without first invoking a password protected screensaver or similar device.
* Users must not in any way cause any form of damage to Turners Occupational Health & Wellbeing Services IT systems and services or the associated hardware.
* Users must comply with any other policies that relate to the use of IT systems and services that Turners Occupational Health & Wellbeing Services may introduce from time to time
	1. Protecting Against Unknown or Malicious Code

Turners Occupational Health & Wellbeing Services will put in place appropriate measures to protect against the possible risk of unknown or malicious code infecting devices, these protective will include:

* Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.
* A combination of proactive measures must be used to help manage the risk of malicious code being run on Turners Occupational Health & Wellbeing Services IT systems and services. A combination of the following measures is recommended:
	+ Deploying antivirus software developed by a reputable supplier, which should be kept fully up to date and used to scan all files: downloaded from the internet, received as attachments to email (or other forms of messaging) and all removable media when inserted.
	+ Advising computer users to avoid running software or opening files obtained from untrusted sources and to be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media.
	+ Managing support of computers such that privilege to install software is restricted to experienced computer support staff.
	1. Backups
* Any essential information stored on a laptop or on a PC’s local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.
* Information system managers are responsible for ensuring that backup arrangements published, or agreed with users of the system, are reliably implemented and that users are informed promptly should there be any problems with, or changes to, the backup arrangements.
1. **Bring Your Own Device**
	1. Introduction
* This section is intended to address the use in the workplace by users of non-Turners Occupational Health & Wellbeing Services owned IT devices such as smart phones, tablets and other such devices to access and store Turners Occupational Health & Wellbeing Services information, as well as their own. This is commonly known as ‘bring your own device’ and referred to in the rest of this policy as BYOD. The use of BYOD devices to process Turners Occupational Health & Wellbeing Services information and data creates issues that need to be addressed particularly in the area of data security.
* Turners Occupational Health & Wellbeing Services must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. As a user you are required to keep secure Turners Occupational Health & Wellbeing Services information and data. This applies equally to information held on Turners Occupational Health & Wellbeing Services IT systems and services and to information held on an employee’s own device.
* Users are required to assist and support Turners Occupational Health & Wellbeing Services in carrying out its legal and operational obligations with regard to Turners Occupational Health & Wellbeing Services data and information stored on your device. Users are required to co-operate with officers of Turners Occupational Health & Wellbeing Services when they consider it necessary to access or inspect Turners Occupational Health & Wellbeing Services data stored on your device.
	1. Scope
* This section applies to all users of Turners Occupational Health & Wellbeing Services IT Systems and Services.
* This section is to ensure that users understand their role and responsibilities when using BYOD and data offsite and accessing Turners Occupational Health & Wellbeing Services IT systems and services from remote locations.
* This section relates to storing and access to Turners Occupational Health & Wellbeing Services information on a BYOD
* Using BYOD devices.
* Using BYOD from Turners Occupational Health & Wellbeing Services premises.
	1. Using BYOD in relation to Turners Occupational Health & Wellbeing Services Systems and Services Off Premises
* All BYOD devices should be password protected.
* Any mobile device which is not protected by a password/pin will not be allowed access to Turners Occupational Health & Wellbeing Services systems.
* BYOD devices used to access Turners Occupational Health & Wellbeing Services IT systems and services which are at risk of malware infection should run anti-virus software.
* Users should not store or access personal, confidential or commercially sensitive information on or from any device not owned by themselves or Turners Occupational Health & Wellbeing Services
* Any potential breach of the General Data Protection Regulation or loss of commercially sensitive data should be notified to Turners Occupational Health & Wellbeing Services ’s Data Manager or Data Protection Officer as soon as possible.
* If a domestic wireless solution is used at the user’s premises, it must be made secure, utilising the wireless security features and password included with the wireless solution, to ensure no unauthorised access is permitted.
* When using BYOD devices to access Turners Occupational Health & Wellbeing Services IT Systems and Services it is the responsibility of remote users to ensure that all reasonable measures have been taken to secure the remote machine. This includes the use of physical or software firewalls, ensuring the device operating system and all software supported by the publisher and is patched and up to date.
* Turners Occupational Health & Wellbeing Services reserves the right to request that personal data on a BYOD device that is the responsibility of Turners Occupational Health & Wellbeing Services be deleted.
* Should Turners Occupational Health & Wellbeing Services introduce/change ‘Mobile Device Management’ software, users must adopt the new software to continue using Turners Occupational Health & Wellbeing Services services on such devices.
* Turners Occupational Health & Wellbeing Services reserves the right to withdraw support of BYOD.

Acceptable Use Policy

Acceptable Use Policy (Staff)

**Computers** and the **Internet** are available primarily to support the functions of the job role. In instances where an individual’s use of a Turners Occupational Health & Wellbeing Services computer or the internet is deemed irresponsible or inappropriate, access to Turners Occupational Health & Wellbeing Services network will be removed for a period of time while the matter is investigated. Be aware that Internet searches and online activities are logged.

**Turners Occupational Health & Wellbeing Services provided Mobile Phones** are primarily used to support the job role and provide effective operation of Turners Occupational Health & Wellbeing Services . You should use your Turners Occupational Health & Wellbeing Services provided mobile phone responsibly and not for personal/social communication or gaming.

The ethos at Turners Occupational Health & Wellbeing Services should make it apparent that a range of activities are absolutely prohibited when IT equipment is used. These activities include:

1. Sending, receiving or displaying offensive/obscene messages or images
2. Using IT to in any way harass, insult, embarrass or attack others
3. Using IT to ‘hack’ into others’ personal files. E.g. email, Turners Occupational Health & Wellbeing Services records or private user-area/profile
4. Obtaining/using accounts or passwords of others when making use of any form of IT
5. Using IT to copy material or otherwise violate laws of copyright
6. Using obscene or offensive language/images when communicating
7. The deliberate damage or corruption of computers, systems or network peripherals

IT Guidelines (Staff)

1. Keep your password secure. Do not tell anyone what it is. Change it regularly. If you suspect your password has been obtained by somebody else, you must inform IT Services ASAP.
2. A secure network is provided to the benefit of all. Respect the safeguards in place and do not attempt to bypass filters or user permissions, this activity will be logged. In particular do not use VPN tunnels, Proxy Servers or non- Turners Occupational Health & Wellbeing Services Internet Services to access blocked material. If a legitimate website is blocked please contact the data manager: tracy@tracyturnerltd.co.uk.
3. If you are using a computer and you find something suspicious, unpleasant or offensive please inform IT Services immediately. Be aware that Internet searches are logged.
4. Never give out personal information (including photos/videos/email address) to anyone you do not know. Never share your password with anyone, including friends or family. Data security at Turners Occupational Health & Wellbeing Services is a collective responsibility.
5. If you receive a request asking you for any personal information, especially via email – stop, think and if unsure report it to IT Services. It is extremely rare for an official provider to require you to send personal information online. Banks, PayPal, HMRC etc will either call or post a formal letter to which it is recommended you call back on a standard number to validate.
6. Do not open attachments if you are unsure of their content. If you don’t know what an attachment might contain, and you were not expecting to receive it please contact the Data Manager.
7. Save your work regularly and backup all of your important files to your allocated private network share, particularly any work you store locally to your own device(s). If you save work to external media, it is your responsibility to keep it safe and avoid loss. Any loss/theft must be reported ASAP. Cloud storage is now a viable alternative to USB drives.
8. Avoid wasting file server storage. Please delete any out of date, duplicated or unwanted files. Turners Occupational Health & Wellbeing Services reserves the right to delete non work-related material from the network drive if we are running low on space. We strongly advise your personal files to be stored on non-networked devices or personal cloud drives.
9. When using a Turners Occupational Health & Wellbeing Services device remember to close down and log off your session correctly. Never leave a device logged in/unlocked when you are not present.
10. Copying software and/or music/movie files is illegal. Please respect the rights of authors and do not copy from any source without official permission this includes Turners Occupational Health & Wellbeing Services network. Those who do are liable for prosecution.
11. Think before you print, save paper whenever possible. Print job log files are retained. Shred any paper documents that are no longer required.

**General Data Protection Regulation**

The GDPR establishes standards for the handling of personal data (data which identifies, or could be used to identify, a natural person). Principally the regulation is concerned that data is handled “lawfully, fairly and in a transparent manner” and protected “against unauthorised or unlawful processing and against accidental loss”. You have a duty to help protect personal data held and used by Turners Occupational Health & Wellbeing Services and to use personal data only for the purposes intended and approved by Turners Occupational Health & Wellbeing Services .

Staff should note that unauthorised disclosure and in particular any deliberate breach by a member of staff may be treated as a disciplinary matter and may be considered gross misconduct in some cases, serious breaches may lead to dismissal.

No set of guidelines can cover all possible situations, staff must use their own judgement to protect personal data and seek advice when unsure.

Along with the existing liabilities for illegal disclosure of data, there are two new criminal offences for which you may be held personally responsible by a court:

* It is an offence to knowingly erase or alter personal data which is currently part of a request under a data subject’s right to access.
* It is an offence to re-identify data which has been treated with a technique to prevent identification of the data subject (i.e. to “de-anonymise” data which has been “anonymised”).

Please follow the guidelines below to help ensure data is handled appropriately:

1. Personal information must not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.
2. If you become aware of a breach of data protection you must report it immediately to The Data Manager or the Data Protection Officer.
3. If you receive a query about what data, we hold or a request about someone’s rights with respect to personal data please contact The Data Manager without delay.
4. Do not use data collected for one purpose for any other purpose without checking with the Data Manager that this is lawful.
5. Do not retain personal data which you no longer require:
	* Check if there are any specific retention policies for your areas of responsibility.
	* Go through your outlook contact list at least once a year and delete contacts you no longer need.
	* Go through your emails at least once a year and delete those no longer relevant.
	* Go through your stored files at least once a year and delete those which you no longer need.

N.B. Turners Occupational Health & Wellbeing Services may have a legal obligation to retain certain records (contact The Data Manager if you need further advice).

1. Do not share data with colleagues unless necessary and do not seek or accept access to data you do not need to complete your professional responsibilities. If in doubt, ask your supervisor or contact The Data Manager for advice.
2. Do not accept personal data you do not need. If you are sent personal data which is unnecessary, irrelevant or inappropriate delete it immediately.
3. Do not transfer personal data from Turners Occupational Health & Wellbeing Services computers or networks to other networks, cloud storage or non-Turners Occupational Health & Wellbeing Services memory sticks, laptops, tablets or mobile telephones, unless specifically authorised in writing.
4. Email to addresses outside the “@turnersoccupationalhealth.co.uk” domain should not include personal data beyond simple contact information (name, email, telephone, job title and place of work). If more extensive data needs to be provided, please use an encrypted attachment (MS Office encryption is adequate for low risk data) or contact The Data Manager about secure transfer options.
5. Do not include the password for an encrypted attachment in the same email and preferably use a different communication method to send the password (e.g. SMS).
6. Emails sent from “@turnersoccupationalhealth.co.uk” addresses to “@turnersoccupationalhealth.co.uk” addresses are restricted to the secure environment and may include personal data.
7. Do not include any personal information in the “Subject” field of email regardless of the recipient.
8. Make it a habit to use “Bcc” rather than “Cc”, “Cc” should only be used where it is necessary for all recipients to see replies.
9. When using Distribution Lists to send emails to those outside Turners Occupational Health & Wellbeing Services , ensure that email addresses are not shared. Use the “Bcc” facility so that email addresses are not displayed.
10. If you wish to use your personal mobile phone for Turners Occupational Health & Wellbeing Services email you must obtain permission from The Data Manager in advance. The Data Manager will require you to ensure your mobile phone is PIN protected and has an application installed which allows remote deletion of data if the device is lost or stolen.
11. Do not leave paper copies of documents containing personal data unsecured, use locked file cabinets whenever possible and if you need to leave your office temporarily unattended whilst working with such documents you must close and lock the office door.

# PROCESSES & PROCEDURES

Data Subject Rights Process

1. **Legal Warning**

Personnel are reminded that knowingly altering or erasing data which is the subject of a “data subject access request” under Articles 13 & 14 of GDPR is a criminal offence.

1. **Responsibility**

Responsibility for ensuring the rights of data subjects are respected and responded to in a timely and appropriate way lies with the Director(s) of Turners Occupational Health & Wellbeing Services .

Day to day management of subject rights is to be delegated to the Data Management Office (DMO).

1. **Data Management Office (DMO)**
	1. Composition

Individual staff may be appointed or removed from participation in the DMO as considered necessary by the Director(s). Initially the DMO will consist of:

* Tracy Turner – tracy@turnersoccupationalhealth.co.uk

All staff will be informed that any request they receive which might be related to data subject rights should be forwarded to the email address above.

* 1. Duties of the DMO

The DMO will on yearly basis:

* Review and approve the processes of Turners Occupational Health & Wellbeing Services regarding data subject rights.

For each request the DMO will:

* Receive and log the data subject request
* Decide on the appropriate level of proof of identity
* Obtain and record the proof of identity
* Clarify and document the nature of the request
* Decide if the request is to be rejected
* Manage the process of satisfying the request including logging all actions and decisions
* Set the redaction policy and process for the request
* Approve any communication with the data subject
1. **Receipt and log of requests**
	1. Obligations of the data subject

Turners Occupational Health & Wellbeing Services recognises that data subjects are under no obligation:

* To have any understanding or knowledge of GDPR
* To understand the specific nature of their rights
* To present a request in any specific form
* To present a request by any prescribed method

Data subjects are obliged to:

* Provide proof of identity if requested
* Provide any information required to identify and locate the relevant data
* Provide reasonable assistance to the controller where required
	1. Staff action on receipt of an enquiry

In consequence of the lack of obligations on the data subject Turners Occupational Health & Wellbeing Services may receive a valid request by any method including but not limited to: telephone, email, physical mail or person interaction.

The request may be presented to any member of staff.

The data subject request does not have to state that it is a request related to the subject’s rights, refer to data protection, privacy or GDPR or satisfy any other requirement.

Therefore, staff need to be trained to:

* Recognise that a request may be related to a data subjects’ right
* Where appropriate, collect suitable contact information
* That it is not necessary at first contact to attempt to clarify the precise details of the request
* Not to attempt to formally identify the data subject
* Not to attempt to satisfy a request themselves
* Forward any request or any enquiry which might be a request to the DMO by email
	1. DMO actions on receipt of an enquiry

When informed of a potential request the DMO will:

* Log the enquiry in the Data Subject Request Log
* Determine if the enquiry is a request under the data subjects’ rights
* Determine if an extension to the deadline is required
* Decide on the redaction policy
* Delegate responsibility for actions and set deadlines for completion
* Update the Data Subject Request Log
* Monitor performance of actions
* Review all communications with data subject
* Sign off completion of request
1. **Identification**
	1. Principles

Turners Occupational Health & Wellbeing Services will not have a pre-set standard for the level of proof of identity required of a data subject.

The level of proof of identity required will be determined with consideration of the following factors:

* If the data relates to a child or vulnerable person
* If the data includes any special category data under Article 9 of GDPR:
	+ Racial or ethnic origin
	+ Political opinion
	+ Religious of philosophical belief
	+ Trade union membership
	+ Genetic data
	+ Biometric data
	+ Health
	+ Sex life or orientation
* If the data includes any data that falls under Article 10 of GDPR:
	+ data regarding criminal convictions
* If the data could be used to assist with identity theft or financial fraud
* If the data relates to a Politically Exposed Person, High Net Worth Individual or Notable Public Figure
* If there is any reason to suspect the person presenting the request may be misrepresenting themselves or there is a more than normal potential that this is the case
* If the data could cause a person to suffer discrimination
* If the data could cause a person to suffer physical harm
	1. Levels of proof of identity

Standard for proof of identity will be based on the HMG Good Practice Guide to Identity Proofing and Verification of an Individual [[HMG Guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720963/good_practice_guide_45_identity_proofing_version_3_february_2017.pdf)]

* + 1. Level One Evidence

A Level 1 Identity is a Claimed Identity with some checks that support the

existence of that identity. The steps taken determine that the Applicant may be the owner of the Claimed Identity.

* Requestor is able to provide details about pre-shared or known facts which it is reasonable to assume would only be known to that individual (two questions minimum)
* Requestor is personally known to a staff member prepared to confirm their identity in writing
* Requestor can be contacted on a fixed line telephone number previously provided by the data subject
* Communication came from a source known by Turners Occupational Health & Wellbeing Services to have been used by the individual on previous occasions (e.g. email address)
	+ 1. Level Two Evidence

A Level 2 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity. The steps taken determine that the identity relates to a real person and that the Applicant is, on the balance of probabilities, the rightful owner of the Claimed Identity.

Two of the following:

* Firearm Certificate
* DBS Enhanced Disclosure Certificate
* HMG issued convention travel document
* HMG issued stateless person document
* HMG issued certificate of travel
* HMG issued certificate of identity
* Birth certificate
* Adoption certificate
* UK asylum seekers Application Registration Card (ARC)
* National 60+ bus pass
* An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)
* An education certificate gained from a well-recognised higher educational institution
* Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)
* Police warrant card
* Freedom pass
* Marriage certificate
* Fire brigade ID card
* Any document listed under level three
	+ 1. Level Three Evidence

A Level 3 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken determine that the identity relates to a real person and that the Applicant is, beyond reasonable doubt, the rightful owner of the Claimed Identity.

One evidence satisfying Level Two and one of the following:

* Passports that comply with ICAO 9303
* EEA/EU full driving licences that comply with European Directive 2006/126/EC
* EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004
* Northern Ireland Voters Card
* US passport card
* Digital tachograph card
* Armed forces ID card
	+ 1. Level Four Evidence

Level Four Evidence cannot be validated by Turners Occupational Health & Wellbeing Services , however under exceptional circumstances a documented decision may be made by the DMO to require additional evidence to establish identity.

1. **Clarification and documentation of the request**

The DMO will determine if the request is of sufficient specificity to be acted on “as is” or if the request requires further clarification.

By default, the DMO will contact the subject with the request form provided in Appendix 2 edited to reflect the level of proof of identity determined to be necessary.

1. **Determination if right exists**

The DMO will decide if the requestor has the right requested and, if not, whether there is a compelling reason to refuse the request. This decision will be documented and recorded in the Data Subject Request Log.

Reasons a requested right may not be available include but are not limited to:

* Turners Occupational Health & Wellbeing Services has a legal obligation to retain data that they are requested to erase
* Data does not constitute “Personal Data” as defined by Article 4 (1) of GDPR
* Release of the data would adversely affect the rights and freedoms of others
* A DPIA or Balancing Test has been conducted which establishes the interest of Turners Occupational Health & Wellbeing Services in processing the data outweigh the risks to the rights and freedoms of the subject who has objected to the processing, requested restriction of processing or erasure of the data
* Request is manifestly unfounded or excessive (in particular because of the repetitive character of the request) as per Article 12 (5) of GDPR and subject refuses to pay a reasonable fee

However, even where it is determined that the subject does not have an enforceable right the request will nevertheless be considered by the DMO and reasons for refusal will be documented.

1. **Refusal of request**
	1. Manifestly Unfounded Request

A request is manifestly unfounded where it “very obviously has no basis and is unjustified”. In such a case a reasonable administration fee may be charged. The reasons for making this decision should be documented and may include:

* Lack of an existing relationship with the subject and no reasonable cause to believe Turners Occupational Health & Wellbeing Services holds data about the subject
* Known antagonistic relationship or grudge
* Data requested does not satisfy the definition of personal data as per Article 4 (1) of GDPR
* Request is part of a repetitive pattern
* Request is clearly a “fishing expedition”

Where a request is judged Manifestly Unfounded the subject must be informed of the reasons for this decision **and** the proposed fee.

* 1. Excessive Request

Subject requests are to be considered a normal part of business since the advent of GDPR and therefore Turners Occupational Health & Wellbeing Services should not be expecting to charge an administration fee for most requests.

Given the above, the fact that there are costs in terms of the time for staff to administer the rights process and collect or erase data or otherwise act to satisfy the request will not be considered excessive for most requests.

It would be reasonable to assume that a request would require in total several hours of time spread among a number of staff of different levels of authority (and therefore expense). However, a total of up to half a day (nominally 4 hours) would be unexceptional and therefore non-chargeable.

An “excessive” request would be a request which considerably exceeded the above i.e. would require more than (perhaps) one day of staff time. Likely reasons include:

* Large volume of data
* Data requires extensive redaction
* Data not on live systems (back-up tapes, archives, etc)
* Request includes hard copy data
* Nature of data requires specialised search techniques

Note that an excessive request still needs to be met if the subject is prepared to pay a reasonable administration fee. Such a fee should reflect the real costs of meeting the request which should be documented to the extent possible.

Where a request is judged excessive the subject must be informed of the reason for this decision.

As a general policy a judgement that a request is excessive should be presented to the data subject in a cooperative way and viewed as the beginning of a potential negotiation as to what data could reasonably be provided free of charge or what data could be excluded to reduce the administration fee.

* 1. Non-Personal Data

Personal data is data which relates to an identified or identifiable natural person. Data **not** falling within this definition is not relevant under GDPR and any decision about releasing such data is outside the scope of this document.

* 1. Adverse Effect on the Rights and Freedoms of Others

Complete redaction of all data about any natural person other than the data subject would frustrate the intent of Article 15 of GDPR (Right of Access).

Therefore, it should not be considered that wherever data about another natural person is included in the data requested this should necessarily be redacted. Data should only be redacted where it could have an adverse effect on the rights and freedoms of others.

Consent may be sought to release data even if there is a high risk of adverse effects.

Factors which may lead to a conclusion that a data item may have an adverse effect:

* Data could result in discrimination or physical harm e.g. racial or ethnic origin, religious or philosophical beliefs, health (disabilities), criminal convictions
* Data relates to a child or vulnerable person
* Data relates to a politically exposed person, high net worth individual or notable public figure
* Release of data would likely be regarded by the other natural person as unwarranted or intrusive
* Data is relevant to a current or likely legal action
* Known facts regarding the relationship between the data subject and the other person

Factors which may lead to a conclusion that a data item may **not** have an adverse effect:

* Other person was party to the original communication in which the data is included e.g. other person’s email addresses in “To” list of emails
* Data is already publicly available e.g. organisation directorships listed at Companies House
* Data is of very low risk e.g. name or email address
* Data subject was in possession of the data at some previous time
1. **Deadline**
	1. Initial Deadline

One receipt of a request the DMO will determine the initial deadline for satisfying the request according to the following criteria:

1. The deadline will be one calendar month from receipt of the request unless criteria 2, 3 or 4 apply e.g.

request received: 25 March

deadline: 25 April

1. Date obtained by adding one calendar month to date of receipt of request falls on a non-working day (weekend or bank holiday) then next working day e.g.

request received: 25 March

add one calendar month: Sunday 25 April

deadline: Monday 26 April

1. Date obtained by adding one calendar month to date of receipt does not exist then last day of month e.g.

request received: 30 January

add one calendar month: 30 February

deadline: 28 February

1. Date obtained from criteria 3 falls on a weekend or bank holiday e.g.

request received: 31 January

add one calendar month: 31 February

last day of month: Saturday 28 February

next working day: Monday 2 March

deadline: 2 March

* 1. Extension

On receipt of a request the DMO will determine if it is reasonable to extend the deadline for satisfying the request by a further two months according to the complexity of the request and if it is decided an extension is appropriate the DMO will document the rationale for this decision and inform the data subject.

The extended deadline will be calculated in the same manner as the initial deadline.

1. **Redaction policy and process**
	1. Redaction Process

The DMO will either nominate the individual (or group of individuals) responsible for performing redaction of personal data or will nominate an individual to make this determination.

Factors to be considered in deciding who to nominate to perform redaction will include:

* Knowledge of the business area the data relates to - e.g. HR data should be redacted by an individual with knowledge of HR law and practice
* Exposure of the data to staff who would not normally have access - e.g. health data should not be redacted by general administration staff who normally would have no reason to access such data
* Seniority – redaction should be performed by staff with sufficient experience and authority to make responsible and informed decisions
* Knowledge of data protection law and practice – may require a two-stage redaction process
	1. Redaction Policy

Guidance for redaction of data will be provided to the individual (or group of individuals) nominated to perform this function on a case by case basis with respect to the section “Adverse Effects on the Rights and Freedoms of Others” above.

1. **Approval of communications with the data subject**

Staff shall be informed that all communications with the data subject must be approved by the DMO.

**Appendix 1**

Generalised process workflow for rights processing



**Appendix 2**

Personal Data – Subject Access Request Form

Please complete this form if you would like us to supply you with a copy of the personal data which we hold about you. You are entitled to receive this information under Data Protection Legislation.

Once completed, please return this form to Turners Occupational Health & Wellbeing Services Data Management Office at the below address:

Turners Occupational Health & Wellbeing Services

3 Queens Square

Attleborough

NR17 2AE

tracy@turnersoccupationalhealth.co.uk

We will endeavour to respond promptly to your request and in any event within one month of the latest of the following:

* Our receipt of this request; or
* Our receipt of any further information from you, which is required to enable us to consider your request.

If, once you have received the requested information, you have any queries or comments, you should contact the Data Management Office at the above postal address or email.

**PART 1: Person the request relates to**

Full name: ………………………………………………………

Date of Birth: …………………………

Address: ……………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………………………………………….

Other relevant addresses during the period to which the personal information relates

……………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………………………………………….

Email address ……………………………..

Mobile phone ……………………………….

These details will only be used for the purpose of dealing with your request.

**PART 3: Proof of identity and address**

Please provide your Customer Identification Number with your name, address and date of birth. If you do not have a Customer Identification Number, please provide copies of the following:

* [As determined by Level of Identity Verification]

We are not obliged to accept any copy documents and may ask to see the originals.

We will retain copies of any documents we receive for a period of [6 months].

**PART 4: Information requested**

To help us to deal with your request quickly and efficiently please provide as much detail as possible about the information you want. If possible, restrict your request to a particular service, department, teams or individuals or incident. Please include timeframes, dates, names or types of documents, any file reference and any other information that may enable us to locate your information, for example, for emails, the names of senders and recipients and approximate dates.

…….…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..

Please note that personal information has different retention periods. If your request relates to CCTV, please state this clearly because the footage may be overwritten after a short period, depending on the storage available.

**PART 5: Method by which the information is to be sent**

If you request the information to be sent by email, the file will be encrypted, and we will send the password to you by text or post.

If you request the information to be sent by post on a CD/DVD or USB, the file will be encrypted, and we will send the password to you separately by text or email.

Please confirm how you wish the personal information to be provided to you, by:

post at the address provided above

email at the email address provided above

These details will only be used for the purpose of dealing with your request, including sending the information and any required passwords.

**PART 6: Supplemental Information**

Would you just like to receive the above information, or would you like the following supplemental information (please tick all that apply):

* + the purposes of processing your personal information
	+ the categories of personal information processed by us
	+ the categories of recipients to whom we disclose your personal information
	+ the envisaged retention period for your personal information
	+ automated decision-making, including profiling, to which your personal information is subject
	+ the source of your personal data, if known

If you believe the information, we hold about you is incorrect, you have the right to ask us to rectify or erase your personal information, to object to its processing or to restrict its processing.

If you are not satisfied with the way in which we have handled your complaint, please contact our Data Management Office at tracy@tracyturnerLtd.co.uk.

If we are unable to resolve the issue to your satisfaction, you have the right complain to the Information Commissioner.

**Please be aware that if you provide false or misleading information, you may be committing a criminal offence.**

I ……………………………………………, confirm that the information provided on this form is correct and that I am the individual whose name appears on this form. I understand that Turners Occupational Health & Wellbeing Services must confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal information I want. I also understand that my request will not be valid until all of the information requested is received by Turners Occupational Health & Wellbeing Services .

Signed: ……………………………………………… Dated: …………………………………

**Breach Process**

Breach Process

Personal Data Breach Process

* 1. **Purpose**

Turners Occupational Health & Wellbeing Services (“we”/”us”) have this procedure in place to provide a standardised response to any reported data breach incident and to ensure that data breaches are appropriately logged and managed in accordance with data protection law and best practice.

* 1. **Scope**

This procedure applies in the event of a personal data breach and applies to all employees of Turners Occupational Health & Wellbeing Services at all times whether located within the physical offices or not.

The document applies to all information we process, and all information technology systems utilised by us.

* 1. **Responsibility**
	2. All employees/staff, contractors or temporary employees/staff and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.
	3. All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Manager who’s contact details are as follows:

Name: Tracy Turner

Telephone: 07818 052507

Email: tracy@turnersoccupationalhealth.co.uk

* 1. **Definition**

The GDPR defines a “personal data breach” in Article 4(12) as: “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”. Examples include:

* Loss or theft of data or equipment on which data is stored
* Access by an unauthorised third party
* Sending personal data to an incorrect recipient
* Alteration of personal data without permission
* Loss of availability of personal data such as equipment failure
* Unforeseen circumstances such as a fire or flood
* Hacking attack
* ‘Blagging’ offences where information is obtained by deceit for the purposes of this procedure data security breaches include both confirmed and suspected incidents.
* Unlawful processing of personal data

\*If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach please refer the matter to the Data Manager for consideration\*

* 1. **Reporting an incident**
	2. Any individual who accesses, uses or manages information within our organisation is responsible for reporting data breach and information security incidents immediately to the Data Manager.
	3. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
	4. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.
	5. **Next Steps**
	6. The Data Manager will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
	7. An initial assessment will be made by the Data Manager in liaison with relevant persons (which may include IT services) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).
	8. An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.
	9. The Data Manager will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
	10. The Data Manager will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
	11. The Data Manager will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.
	12. The Data Manager will also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.
	13. **Procedure – Breach notification processor to controller**
	14. Turners Occupational Health & Wellbeing Services must report any personal data breach or security incident to the controller without undue delay. These contact details are recorded in the Breach Register. Turners Occupational Health & Wellbeing Services provides the controller with all of the details of the breach.
	15. The breach notification should be made by email and/or phone call.
	16. A confirmation of receipt of this information should be requested and made by email and/or phone call.
	17. **Procedure – Breach notification controller to supervisory authority**
	18. The Data Manager will determine if the supervisory authority (the Information Commissioner’s Office (ICO in the UK) need to be notified in the event of a breach.
	19. If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The Data Manager will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.
	20. We will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment. If we decide that we do not need to report the breach to the ICO we will justify and document our decision.
	21. If a risk to data subject(s) is likely, the Data Manager will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.
	22. If the data breach notification to the ICO is not made within 72 hours, the Data Manager will submit notification electronically with a justification for the delay.
	23. If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.
	24. The following information needs to be provided to the supervisory authority:
		+ A description of the nature of the breach.
		+ The categories of personal data affected.
		+ Name and contact details of the Data Manager.
		+ Likely consequences of the breach.
		+ Any measures taken to address the breach.
		+ Any information relating to the data breach.
		+ Approximate number of data subjects affected.
		+ Approximate number of personal data records affected.
	25. The breach notification should be made via telephone - **ICO: 0303 123 1113.** Alternatively, the Data Managermay choose to [report it online](https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc) if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.
	26. In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.
	27. **Procedure – Breach notification controller to data subject**
	28. If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Turners Occupational Health & Wellbeing Services will notify the data subjects affected without undue delay and in accordance with the Data Manager’s recommendation.
	29. A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. In any event the Data Manager will document their decision-making process.
	30. We will describe the breach in clear and plain language, in addition to information specified in clause 8.7.
	31. The controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
	32. If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the Data Manager whose decision will be final.
	33. If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Turners Occupational Health & Wellbeing Services will communicate the data breach to the data subject(s) by telephone or email.
	34. We will document any personal data breach within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action taken.
	35. **Documentation requirements**

Turners Occupational Health & Wellbeing Services will complete a record in the Breach Register for all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under DPA 2018. Part 3, Chapter 4 (67) requires an organisation to document the facts relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability principle and allows us to verify the organisation’s compliance with its notification duties under the DPA 2018.

* 1. **Evaluation**
	2. Once the initial incident is contained, the Data Manager will carry out a full review of the causes of the breach; the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken.
	3. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.
	4. The review will consider various points, including but not limited to:
* Where and how personal data is held and where and how it is stored
* Where the biggest risks are, and identify any further potential weak points within its existing measures
* Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
* Staff awareness

# NOTIFICATIONS

Notifications to Data Subjects

**Turners Occupational Health & Wellbeing Services Privacy Notifications**

# Background

With the specific requirements of GDPR Articles 12-14, one notification (policy) that covers all categories of data subject which Turners Occupational Health & Wellbeing Services processes data about would necessarily become rather cumbersome and complicated and thus would not meet Article 12’s requirement to be “*concise, transparent and easily accessible . . . using clear and plain language*”.

It is proposed that individual notifications are prepared for each category of data subject and a web page is provided with links to these notifications with text similar to:

Privacy Notice

Thank you for using tracyturnerltd.co.uk. Here, we explain what personal information we may hold about you, and how we might use that information.

Please note that where our website contains links to other websites, we are not responsible for the privacy policies of other organisations and websites. This policy applies solely to any personal information collected on tracyturnerltd.co.uk.

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3 Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email tracy@turnersoccupationalhealth.co.uk

To contact our Data Protection Officer email DPO@priviness.eu

information we collect

Personal information is any information that can be used to identify a living individual. Through the contact form on our website we collect your name, email address, and telephone number, in addition, if you complete a review form, we will also collect your opinion about our services. Any personal information that you provide us via our website is stored securely. We may collect this personal information when you contact us, or otherwise give us personal information. We do not collect any personal information about you on our website that you do not give us.

How do we use this information?

We use your personal information you have provided to us via our website in a number of ways:

* In our legitimate interest in communicating with you to provide you with the information you ask for, for example contacting you about a service offer of which you have requested information. We will retain this information for up to 12 months after our last contact with you, unless you request that we delete the data beforehand.
* If you complete a review form, we may post that review on our website or our company literature in our legitimate interest to promote Turners Occupational Health & Wellbeing Services . Such data will be retained for up to 2 years, unless you request that we delete the data beforehand.

We will also use your personal information to ensure that content from our site is presented in the most effective manner for you and for your computer and to carry out our obligations arising from any contracts entered into between you and us. In addition, we may handle any non-sensitive personal data for our legitimate purposes.

We will not sell your details to any third parties or use your data in any other way than those listed above.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Turners Occupational Health & Wellbeing Services regards the lawful and correct handling of personal information as important to the success of our work and to maintaining the confidence of those with whom we deal. We will ensure that anyone working for us uses personal information lawfully and correctly. To this end, we will ensure we fully comply with data protection legislation.

How we use cookies

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. On our website, unlike many others, we only use cookies that are essential to the running of the website and therefore whilst we do not require your consent to use such cookies we do believe in transparent and honest communications. So that you are aware of what cookies are being placed on your computer we have produced the table below to show each cookie and explain what it does.

|  |  |  |
| --- | --- | --- |
| Cookie | Type | Purpose |
| bongodeletecookiemsg | Essential | This cookie controls the cookie message bar on the web page, making it appear or hide as selected by you |

Your Rights

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@turnersoccupationalhealth.co.uk.

If you wish to make a complaint about how we have handled your personal data, please email info@tracyturner.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

To view your privacy notice regarding our processing of personal data concerning you, please choose from below the category which most closely describes your relationship with Turners Occupational Health & Wellbeing Services :

* Employee
* Recruitment Candidate
* Workers
* Private Clients
* Email/ Business Contact

|  |
| --- |
|  **Data Privacy Notice** |

**Data Subject: Employee**

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3,Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email info@turnersoccupationalhealth.co.uk

As an employee of Turners Occupational Health & Wellbeing Services, we hold the following information about you:

* Contact details
* Date of Birth
* Gender
* Payroll details
* Banking details
* Pension details
* Tax details
* Salary
* Expenses
* Contract details
* Certifications
* Appraisal and Development Plans
* Absence Records
* Right to Work documentation

This data may come directly from you or be generated by Turners Occupational Health & Wellbeing Services .

We hold and process this data for the purposes of the performance of the contract of employment, including discharge of obligations laid down by law, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work and for the purposes of the exercise and enjoyment of rights and benefits related to employment and for the purpose of the termination of the employment relationship.

If we are unable to process this data, we would not be able to continue with our contract of employment with you.

We may transfer certain data to our payroll provider as necessary to make payments, to see how they use your data you can read their privacy notice by clicking [here](https://www.mapartners.co.uk/privacy-policy/).

We pass certain data on to third parties including, your/our Bankers, insurance companies, local authorities and regulatory bodies when required to do so. We will also provide references to companies and regulatory bodies, as requested by you, when you are applying for employment.

We have a legal obligation to keep certain records related to your employment and may retain these records for up to 7 years from date of termination (for example under: The Finance Act 2008 or the Reporting of Injuries Diseases and Dangerous Occurrences Regulations 2013).

Other data may be kept for up to 5 years from termination of employment in case there are queries about your employment, unless you request that we delete the data beforehand.

Pension related details are kept for 75 years.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@tracyturner.co.uk

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

If you wish to make a complaint about how we have handled your personal data, please email info@tracyturner.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

|  |
| --- |
| **Data Privacy Notice** |

**Data Subject: Recruitment Candidates**

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3,Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email info@turnersoccupationalhealth.co.uk

As potential employee of Turners Occupational Health & Wellbeing Services , we hold the following information about you:

* Name
* Contact details
* CV
* Reference Details

This data may come directly from you or from your previous employer. We hold and process this data for the negotiation of a potential contract of employment with you.

If we are unable to process this data, we would not be able to process your application.

We do not share this data with anyone, nor is it transferred outside of the EEA.

Should you be unsuccessful we will retain this data for up to 6 months so that we may contact you regarding any future opportunities, unless you request that we delete the data beforehand.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@tracyturner.co.uk

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

If you wish to make a complaint about how we have handled your personal data, please email info@tracyturner.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

|  |
| --- |
| **Data Privacy Notice** |

**Data Subject: Workers**

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3, Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email info@turnersoccupationalhealth.co.uk

As a worker for a client of Turners Occupational Health & Wellbeing Services , we may hold the following information about you pertaining to your employment:

* Name
* Contact details
* Health Data
* Health Surveillance Data
* Health Records
* Medical Reports
* Drug and Alcohol test results
* NI Number

This data may come directly from you, your employer, medical professionals or may be generated by ourselves.

Where your employer is of one of our clients we hold and process this data in our legitimate interest in fulfilling the business-to-business contract we have with your employer.

Where it is part of our contract we will offer advice to your employer regarding your fitness to work, however the details of any data about you obtained from testing, your GP, or conversations with you will remain confidential and we will not share such data with anyone without your express consent, unless we are legally required to do so.

Where we may occasionally be required to disclose certain information to additional third parties, we will disclose data only when and to the extent that we have a legal obligation to do so.

Such third parties may include:

* law enforcement (by warrant or subpoena)
* courts, tribunals or other judicial bodies
* the Health and Safety Executive

We have a legal obligation to retain your personal information for up to 50 years, for example under COSHH regulations 2002, or the period of our contract with your employer, whichever is the sooner.

Should our contract with your employer cease, your data will be given to the new Occupational Health provider if you give your consent for us to do so, or to yourself.

Where your personal information is collected on health promotion days or sessions that information is given to you at the time of your session with us and is not used or retained by us in any way.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@turnersoccupationalhealth.co.uk

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

If you wish to make a complaint about how we have handled your personal data, please email info@turnersoccupationalhealth.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

|  |
| --- |
| **Data Privacy Notice** |

**Data Subject: Private Client**

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3, Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email info@turnersoccupationalhealth.co.uk

As a private client of Turners Occupational Health & Wellbeing Services , we may hold the following information about you:

* Name
* Contact details
* Health Data
* Health Surveillance Data
* Health Records
* Medical Reports
* Drug and Alcohol test results
* NI Number

We only obtained this data from yourself and we hold and process this data for the purposes of supplying you with a service, communicating with you and invoicing you so that we can fulfil our contract we have with you. If we are unable to process this data, we would not be able to continue with our contract with you.

We will not share such data with anyone without your express consent, unless we are legally required to do so.

Where we may occasionally be required to disclose certain information to additional third parties, we will disclose data only when and to the extent that we have a legal obligation to do so.

Such third parties may include:

* law enforcement (by warrant or subpoena)
* courts, tribunals or other judicial bodies
* the Health and Safety Executive

We have a legal obligation to retain your personal information for up to 50 years, for example under COSHH regulations 2002, or the period of our contract with you, whichever is the sooner.

Should our contract with you cease, your data will be given to your new Occupational Health provider if you give your consent for us to do so, yourself or retained for storage by ourselves on your behalf with your consent.

Where your personal information is collected on health promotion days or sessions that information is given to you at the time of your session with us and is not used or retained by us in any way.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@turnersoccupationalhealth.co.uk

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

If you wish to make a complaint about how we have handled your personal data, please email info@turnersoccupationalhealth.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

|  |
| --- |
| **Data Privacy Notice** |

**Data Subject: Email Contacts**

For the purpose of data protection legislation, including the UK Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the UK Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation, the controller is:

Turners Occupational Health & Wellbeing Services

3,Queens House

Queens Square

Attleborough

Norfolk

NR17 2AE

Email info@turnersoccupationalhealth.co.uk

As an email or business contact to Turners Occupational Health & Wellbeing Services , we hold the following information about you:

* Name
* Contact details
* Job title
* Company

This data may come directly from yourself, your employer or from another business contact. We hold and process this data for the legitimate interest of communicating with you in the course of our business.

We will retain this data for up to 12 months from our last contact with you, unless you request that we delete the data beforehand.

At the conclusion of all relevant retention periods, physical documents containing your personal data will be shredded, and all personal data held electronically will be deleted.

Data protection legislation states that you have the following qualified rights regarding your personal data:

* Access – you may request we provide you with the data we hold
* Rectification – you may request we correct any inaccurate data
* Erasure – you may request we erase your data
* Restriction – you may request we stop processing your data but retain it
* Portability – you may request we provide you or a nominated party with your data in a commonly used, structured and machine-readable format

You can exercise your rights at any time by using the postal address above or by contacting us at info@turnersoccupationalhealth.co.uk

Any changes we may make to this notification in the future will be posted on this page and where appropriate notified to you by e-mail.

If you wish to make a complaint about how we have handled your personal data, please email info@turnersoccupationalhealth.co.uk and we will investigate the matter.

If you are not satisfied with our response or believe we are not processing your data in accordance with the law, you can contact a National Data Protection Authority which, in the UK is the [Information Commissioner’s Office](https://ico.org.uk/). For a list of other European Data Protection Authorities click [here.](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080)

# REGISTERS & LOGS

# Logging Your Subject Access Requests & Data Breaches

Working excel versions of these documents are available separately





1. The right to data portability applies in the case of contract being the legal basis. [↑](#footnote-ref-1)
2. The right to not being subject to automated decision-making, including profiling, does not apply where there is a necessity for the purposes and legal basis of a contract (or entering into a contract).

The right to data portability applies in the case of contract being the legal basis. [↑](#footnote-ref-2)