Policy Name:	Data Protection
Policy Number:	ICT002
Date of Approval:	June 2001
Effective Date:	June 2001
Revised Date:	June 2023
Review by Date:	June 2025
Policy Author:	Head of Technology
Policy Owner:	Finance and Resources Director
Management Committee Approved By:	TLT
Governor Committee (where appropriate) Approved By:	n/a
For Action By:	All Employees
For Information to:	All Employees
Approval requested to upload on the Treloar's Website:	Yes □ (tick if requested)

Who is carrying out EIA?	TLT	Date of EIA?	April 2018
Have we shown due regard for the 9 protected characteristics within the policy/procedure?		Yes ☑ No ☐	
Are all opportunities to promote equality taken within the policy/procedure?		Yes ☑ No ☐	
Refer Policy/Procedure to EDI Co-ordinator for further assessment		Yes o No ☑	

1. Policy/ Procedure Aim

This policy provides information and guidance to staff about how Treloar's processes and protects personal data and what the employer's and employees' rights and responsibilities are.

This policy applies to all staff, including temporary and bank staff, and contractors.

2. Policy/Procedure Details

General

The UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 is the data protection regime that applies to most UK businesses and organisations. Its purpose is to protect the "rights and freedoms" of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, with their consent.

Treloar's is registered with the Information Commissioner's Office (Z5474271) as a Data Controller. Our data protection entry is amended as and when there are changes in the way Treloar's administers personal records of its staff, students and other individuals eg fundraisers/donors etc.

Compliance with data protection legislation is the responsibility of all employees of Treloar's who process personal data.

This policy includes in its scope all data which we process, whether in hardcopy or digital copy; this includes special category data.

Data Protection Officer

The Data Protection Officer is the Finance and Resources Director at Treloar's. They have been appointed to take responsibility for Treloar's compliance with the policy on a day to day basis and ensure that the rights of staff and students in terms of their personal data are upheld. The Data Protection Officer is the first point of call for staff/students seeking clarification on any aspect of data protection compliance.

The Data Protection Principles

All processing of personal data must be demonstrably conducted in accordance with the data protection principles as set out in Article 5 of the GDPR.

1. Personal data shall be processed lawfully, fairly and transparently. Privacy information will be made available to all staff and students – see

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and limited to what is necessary for processing.
   Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the procession of personal data.

4. Personal data shall be accurate and, wherever necessary, kept up to date, with every effort to erase or rectify without delay.
   It is the responsibility of the data subject to ensure that data held by Treloar's is accurate and up to date. Employees are required to notify HR of any changes in circumstances to enable personal records to be updated accordingly, or make the changes themselves in iTrent Self Service.
   The Data Protection Officer is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is not to be used to inform decisions and for passing any correction to the personal data, where required.

5. Personal data processed for any purpose or purposes shall not be kept for longer than it is necessary for that purpose or those purposes.
   Personal data will be retained in line with ICT03 Retention of Records policy and securely destroyed once the retention date is passed, as set out in this procedure.
   The Data Protection Officer will specifically approve any data retention that exceeds the retention periods defined in ICT03 Retention of Records policy and ensure that justification is clearly identified.

6. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7. Over and above the principles described above, measures shall be put in protect the confidentiality of people's health and care information and making sure it is used properly. To this end a Caldicott Guardian shall be appointed (currently the Director of Finance and Resources) as the senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly and adherence to the Caldicott Principles (see Appendix E).

Data Protection by Design and by Default

We shall uphold the principles of data protection by design and by default, from the beginning of any data processing and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) [1]

All new systems used for data processing will have data protection built in from the beginning of the system change. All existing data processing has been recorded on our Record of Processing Activities (ROPA).

Personal data is only processed when necessary for specific purposes and with the least amount of identifiable data necessary to complete the work it is required for; individuals are therefore protected against privacy risks.We only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it (ICT003 Retention of Records Policy).

Where possible we will use pseudonymised data to protect the privacy and confidentiality of our staff and students.

National Data Opt-Out

Prior to starting any new data processing we assess if the national data opt-out applies. This is recorded in our DPIA.

We do not currently share any information that is not for individual care and treatment. If this changes we will we use MESH to check if any of our staff or students have opted out of their data being used for this purpose.

Employee Rights/Student Rights

We uphold the personal data rights outined in the GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Staff and students may request to view any of their personal records held by the Trust (in digital and/or hardcopy). Formal request should be directed to the Data Protection Officer in writing preferably using the Subject Access Request form (Appendix C: Subject Access Request) although other methods e.g. letter, email, are acceptable.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

The Data Protection Officer is responsible for responding to requests for rectification or access from data subjects within one month. This can be extended to a further 2 months for complex requests. If Treloar's decide not to comply with the request, the Data Protection Officer will respond to the data subject to explain its reasoning and inform them of their right to complain and seek judicial remedy.

The Data Protection Officer will instigate action to rectify or destroy inaccurate data, including the right to be forgotten.

All Subject Access Requests will be logged centrally.

Consent

Treloar's understands 'consent' to mean that it has been explicitly and freely given, and that it is a specific, informed and unambiguous indication of the data subjects' wishes that, by a statement or clear affirmative action signifies agreement to the processing of personal data relating to him or her.

Responsibilities of the Trust and of all Employees

All Employees are responsible for ensuring that any personal data that Treloar's holds is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Treloar's to receive that information and has entered into a confidentiality agreement – see Appendix C: Non-Disclosure Agreement

Advice and Guidance

The Data Protection Officer should be consulted prior to handling, disclosing or transferring personal information held either on computer or other medium. Whenever a new database is required the Data Protection Officer must be informed in order that it may be formally registered with the Information Commissioner.

****

3. Key Responsibilities

Policy/Procedure Communication and Implementation Action Plan - Amend and add to as appropriate		
	Action	Responsibility
1	Ensure that all managers, employees and volunteers of Treloar's have access to the related procedures.	Treloar Leadership Team
2	Train all managers, employees and volunteers in the implementation of the policy and the related procedures.	Human Resources Director (delegated to Training Manager)
3	Ensure that all new employees, staff and volunteers are made aware of the policy, understand it, know where to access a copy and where to access the related procedures.	All Managers
4	Ensure that new employees, staff and volunteers know their responsibilities	All Managers and staff

4. Implications of Policy/Procedure

Training Requirements

All employees will undergo Data Protection training as part of their induction. A refresher course for all staff will take place every 3 years.

Communication Requirements

How will the Policy/procedure be communicated:	Sharepoint	
Who will ensure the above communication is carried out::	PA to Finance and Resources Director	
Do the changes made to this policy/procedure affect any other policies/procedures? If yes, has this been communicated to the policy/procedure author/owner		No

Inclusive Communications

If you require this document in an alternative format, such as large print, audio description, or a coloured background, please contact Jo Cox at jo.cox@treloar.org.uk

5. Monitoring and Review

Every two years or earlier as and when required

6. Links to other related policies, procedures or documents (internal)

CG 054 – Confidentiality of Medical Information and Consent to Treatment
ICT003 – Retention of Records Policy

7. Further sources of information (external)

General Data Protection Regulation 2018
The Data Protection Act 2018

8. Revision History

Listed below is a brief audit trail, detailing amendments made to this policy procedure in last 4 years

Page/para No.	Brief description of the change(s)	Change made by	Date
Whole policy	Transferred into a new template	Finance and Resources Director	17 April 2014
Page 2	Added Aim of the policy Updated the name of the Data Protection Officer Elaborated on the rights/responsibilities of students and staff	Finance and Resources Director	17 April 2014
Page 3	Added reference to Retention of Records Policy	Finance and Resources Director	17 April 2014
Page 4	Changed the way the policy is communicated	PA to FD	6 April 2016
Rewrite	GDPR changes to legislation	Head of Technology	Jan 2018
P4	Reference to IRIS	Head of Technology	02/09/2019
Various	Minor changes to dates and job titles	Head of Technology	06/10/2020
Various	Minor changes	Head of Technology	16/12/2022
Various	Changes relating to DSPT	Head of Technology	22/06/2023

IMPORTANT NOTES:
It is essential for those with designated responsibilities to familiarise themselves with the sources of information, referred to above.

Policy documents describe mandatory minimum standards and will be subject to audit and review. Line managers are required to ensure suitable and sufficient arrangements are in place to meet policy requirements, including the provision of information and instruction to staff.

STUDENT PRIVACY NOTICE

WHAT IS THE PURPOSE OF THIS DOCUMENT?

Treloar's is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after you leave Treloar's, in accordance with the General Data Protection Regulation (GDPR).

It applies to all students, however funded, in School and College.

Treloar's is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former students. This notice does not form part of any contract and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Our Data Protection Officer and data protection representatives can be contacted directly here:

- dpo@treloar.org.uk
- 01420 547400 x 3423

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will collect, store, and use the following categories of personal information about you:

- Personal information (such as name, date of birth, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Next of kin and emergency contact information.
- Other contact information (such as social workers, external healthcare professionals)
- Attendance information, including number of absences and absence reasons
- Educational assessment information and progress against targets set.
- Healthcare assessment information and progress against targets set.
- Relevant medical information, including disability, medication and medical notes
- Medical correspondence and Reports
- Therapeutic information and notes which may include occupational therapy, physiotherapy, speech and language therapy, dietetics, visual impairment and counselling.
- Special educational needs information
- Behavioural information, including exclusions and behaviour support plans
- Care Plan including support and personal care requirements
- Photographs for educational or care purposes
- Funding and payment information (where you are the customer)

WHY WE COLLECT AND USE THIS INFORMATION

- To support student learning
- To keep students safe
- To monitor and report on student progress
- To provide appropriate care, medical and therapeutic support
- To assess the quality of our services
- To comply with the law regarding data sharing

The information you supply is also used by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE), to issue you with a Unique Learner Number (ULN) and to create your Personal Learning Record, as part of the functions of the DfE. For more information about how your information is processed, and to access your Personal Learning Record, please refer to:
https://www.gov.uk/government/publications/lrs-privacy-notices

THE LAWFUL BASIS ON WHICH WE USE THIS INFORMATION

We collect and use student information under the requirements of the Education Act 1996 (school) and the Education and Skills Act 2008 (college) and to satisfy the requirements placed upon us by your Local Authority as a condition of your place with us.
More information can be found here:
School - https://www.gov.uk/education/data-collection-and-censuses-for-schools
College - https://www.gov.uk/government/publications/esfa-privacy-notice

COLLECTING STUDENT INFORMATION

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

STORING STUDENT DATA

We hold student data for 7 years after leaving, or until 25th birthday, whichever is the greater. For students with looked after child status data is held until 75th birthday or 15 years after the date of death, whichever is sooner.

WHO WE SHARE STUDENTL INFORMATION WITH

We routinely share student information with appropriate internal staff and outside healthcare agencies, where deemed appropriate by the Medical Officer, Nurse Manager or Therapy professional(HCPC or NHS registered). In addition we will share

information with:

- Schools/colleges that the student attends after leaving us
- Your local authority
- Department for Education (DfE)
- Health and therapy professionals involved in your care
- On-site GP

HOW WE SHARE STUDENT INFORMATION

We may share personal and sensitive personal information with pre-identified and verified parents/guardians via email. This communication will be unencrypted but kept to a minimum.
Student data that is shared with any other professional body or organisation will be sent via a secure portal or an encrypted email.

WHY WE SHARE STUDENT INFORMATION

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.
We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins our funding and educational attainment policy and monitoring.
We are required to share information about our students with the relevant local authority and the Department for Education under The Education (Information About Individual Pupils) (England) Regulations 2013.

REQUESTING ACCESS TO YOUR PERSONAL DATA

Under data protection legislation, you have the right to request access to the information we hold about you. To make a request for your personal information, or be given access to your educational record, contact Emma Simmonds, Admissions and Contracts Manager - emma.simmonds@treloar.org.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

CONTACT

If you would like to discuss anything in this privacy notice, please contact Emma Simmonds, Admissions and Contracts Manager – emma.simmonds@treloar.org.uk

Appendix B: Staff Privacy Notice (December 2022)

GDPR Privacy notice for employees, workers and contractors (UK)

What is the purpose of this document?

Treloar's is committed to protecting the privacy and security of your personal information.
This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).
It applies to all employees, workers and contractors.

Treloar's is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence and/or passport/and/or other identity documents.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records. This includes information relating to health screening in response to a pandemic.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates

or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies including the Disclosure and Barring Service.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest (or for official purposes).

Situations in which we will use your personal information

We need all the categories of information in the list above (see: *The kind of information we hold about you*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing the following benefits to you: Pension scheme (including salary sacrifice), Independent Financial Advice, Life Insurance, Occupational Health Service, Flu Vaccinations, Cycle to Work Scheme, Childcare Vouchers Scheme, Staff Introduction Scheme, Training and Development, Sick Pay, Special Leave, Health Cash Plan, Perkbox, Employee Assistance Programmes, Critical Illness Cover, Car Parking, Sabbatical Leave, Long Service Awards, Staff Awards.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, supervisions, managing performance

and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- Providing an audit trail of activities performed.
- As part of an individual student's care or academic record or for use as part of a student communication aid.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities/Equality and Diversity monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

”Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our occupational pension scheme), and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members, with the appropriate safeguards, in the course of legitimate business activities and safeguarding issues.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, sexual orientation, disability, age, marital status or civil partnership to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal

information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy, DBS policy and safer recruitment policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities or safeguarding matters with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you or the police in the course of you working for us. We are allowed to use your personal information in this way to carry out our obligations.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

Data sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

If necessary we may transfer your personal information outside the EU (*for example*: *requesting and verifying overseas references, requesting and verifying overseas police checks, working or travelling overseas on Treloar's business*).

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group (such as Treloar Enterprises). The following activities are carried out by third-party service providers: pension administration, benefits provision and administration, employment agencies, volunteering agencies, training providers, apprenticeship providers, access to work and other Government Agencies.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required

to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group (such as Treloar Enterprises) as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise and for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context possible restructuring of the business and employment references. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available on Share Point (ICT02 – Data Protection Policy, ICT03 – Retention of Records Policy, ICT05 – Information Security Policy)
Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any

legal, accounting, insurance, reporting or safeguarding requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available on SharePoint. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Head of HR in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Head of HR. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data protection officer

We have appointed the Finance and Resources Director as data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Simon Birch, Finance and Resources Director, Treloar's or Sandra Faulkner, Head of Human Resources.

I,_____ (employee/worker/contractor name), acknowledge that on
_____ (date), I received a copy of Treloar's Privacy Notice for employees, workers and contractors and that I have read and understood it.
Signature
……

Name (Please print)

……
Job role
……

Once completed please return this document, signed and dated to the HR Department, Treloar's.

Appendix C: Subject Access Request

1. DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Previous address	<required if staff or student member is not current>				
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:	< We will need two copies of forms of identification – these will be destroyed once ID has been approved>				
Details of data requested (including dates if appropriate):					

2. DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their written or other legal authority?	Yes ☐ No ☐
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)	
Please enclose proof that you are legally authorised to obtain this information.	

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					

3. DECLARATION

I, ……, the undersigned and the person identified in (1) above, hereby request that Treloar's provide me with the data about me identified above.

Signature: Date:

Name:

I, ……, the undersigned and the person identified in (2) above, hereby request that Treloar's provide me with the data about the data subject identified in (1) above.

Signature: Date:

Name:

This form must immediately be forwarded to Treloar's's Data Protection Officer.

Appendix D: Non-Disclosure Agreement

One-way Non-Disclosure Agreement

Date: []

Parties:

[NAME OF INDIVIDUAL RECEIVING INFORMATION] of [address of individual] OR **[NAME OF COMPANY RECEIVING INFORMATION]**, a company registered in [England] under company number [number on Register of Companies] whose registered office is at [address of office on the Register of Companies] **(the Recipient)** and
TRELOAR TRUST a company registered in England under company number 4466362 whose registered office is at Holybourne, Alton, Hampshire, GU34 4GL **(the Discloser)**

1. The Discloser intends to disclose information (**the Confidential Information**) to the Recipient for the purpose of [insert details e.g. discussing the possibility of the Recipient and the Discloser entering into a joint venture] **(the Purpose)**.

2. The Recipient undertakes not to use the Confidential Information for any purpose except the Purpose, without first obtaining the written agreement of the Discloser.

3. The Recipient undertakes to keep the Confidential Information secure and not to disclose it to any third party [except to its employees [and professional advisers] who need to know the same for the Purpose, who know they owe a duty of confidence to the Discloser and who are bound by obligations equivalent to those in clause 2 above and this clause 3.

4. The undertakings in clauses 2 and 3 above apply to all of the information disclosed by the Discloser to the Recipient, regardless of the way or form in which it is disclosed or recorded but they do not apply to:

a) any information which is or in future comes into the public domain (unless as a result of the breach of this Agreement); or

b) any information which is already known to the Recipient and which was not subject to any obligation of confidence before it was disclosed to the Recipient by the Discloser.

5. Nothing in this Agreement will prevent the Recipient from making any disclosure of the Confidential Information required by law or by any competent authority.

6. The Recipient will, on request from the Discloser, return all copies and

records of the Confidential Information to the Discloser and will not retain any copies or records of the Confidential Information.

7. Neither this Agreement nor the supply of any information grants the Recipient any licence, interest or right in respect of any intellectual property rights of the Discloser except the right to copy the Confidential Information solely for the Purpose.

8. The undertakings in clauses 2 and 3 will continue in force [indefinitely][for [insert number] years from the date of this Agreement].

9. This Agreement is governed by, and is to be construed in accordance with, English law. The English Courts will have non-exclusive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement.

[If the Recipient is an individual]
Signed and Delivered as a Deed by
[name of Recipient] in the
presence of:

……
Signature of witness

……
Name of witness

……

……

……
Address of witness

[If the Recipient is a company]
Executed and Delivered as a Deed by
[name of Recipient] acting by
[name of director], a director,
in the presence of:

……
Signature of witness

……
Name of witness

……

……

……
Address of witness

Appendix E - Caldicott Principles

First introduced in 1997 and since expanded, are a set of good practice guidelines for using and keeping safe people's health and care data. Caldicott guardians support the upholding of the principles at organisational level. All NHS organisations must have a Caldicott guardian, and a wider range of bodies (including Treloar's) are now expected to have a guardian in place. The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and where they would expect this to be kept private.

- Principle 1: justify the purpose(s) for using confidential information.
- Principle 2: use confidential information only when it is necessary.
- Principle 3: use the minimum necessary confidential information.
- Principle 4: access to confidential information should be on a strict need-to-know basis.
- Principle 5: everyone with access to confidential information should be aware of their responsibilities.
- Principle 6: comply with the law.
- Principle 7: the duty to share information for individual care is as important as the duty to protect patient confidentiality.
- Principle 8: inform patients and services users about how their confidential information is used and what choice they have.