DATA PROTECTION POLICY

Date Updated:	May 2018
Lead persons(s):	Employee Engagement and PSTE
Review date:	Bi annual or when there is a change in statutory guidance or legislation

Contents

1. Aims

The Trust aims to ensure that all personal data collected about staff, pupils/students, parents/carers/guardians, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (**GDPR**) and the expected provisions of the Data Protection Act 2018 (**DPA 2018**).

This policy applies to all personal data, regardless of whether it is in paper or electronic format. References to staff includes current and former employees, workers, volunteers, apprentices and consultants. References to pupils/students includes past and prospective pupils/students.

This policy explains how the Trust will hold and process personal data. It explains staff rights as data subjects and also explains their obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Trust.

This policy does not form part of any contract of employment (or contract for services) and can be amended by the Trust at any time.

2. Legislation and guidance

It is intended that this policy is fully compliant with the DPA 2018 and the GDPR. It is based on guidance published by the Information Commissioner's Office (**ICO**) on the GDPR and the ICO's code of practice for subject access requests. If any conflict arises between those laws and this policy, the Trust intends to comply with the DPA 2018 and the GDPR. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. It includes expression of opinion about the person and an indication of the intentions of the Trust or others. It does not include anonymised data.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
The Trust	Includes the whole of the Ruskin Mill family of organisations: Ruskin Mill Trust Limited, Transform Residential Limited, Clervaux Trust Limited, Brantwood Specialist School Limited, Lantern Trading Limited, Sunfield Children's Homes Limited, Ruskin Mill Land Trust, Ruskin Glass Centre Limited and Academy of Makers Limited.

4. The data controller

The Trust processes personal data relating to staff, pupils/students, parents/carers/guardians, trustees, visitors and others, and therefore is a data controller.

The following entities within the Trust are registered as a data controller with the ICO and will renew their registration annually or as otherwise legally required:-

Entity	**ICO Registration Number**
Ruskin Mill Trust Limited	Z7589083
Transform Residential Limited	Z2720383
Clervaux Trust Limited	ZA223569
Brantwood Specialist School	Z2718500
Lantern Trading Limited	Z2718531
Sunfield Children's Homes Limited	Z7064238
Ruskin Mill Land Trust Limited	ZA014176
Ruskin Glass Centre Limited	ZA223595
Academy of Makers Limited	ZA226258

5. Roles and responsibilities

This policy applies to all current and former employees, workers, volunteers, apprentices and consultants, and to external organisations or individuals working on our behalf (**staff**). Staff should read this policy alongside their contract of employment (or contract of services) and any other notice the Trust may issue from time to time in relation to data. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing boards

The governing boards of each of the organisations within the Trust have overall responsibility for ensuring compliance with all relevant data protection obligations for their particular organisation.

5.2 Data protection officer

The data protection officer (**DPO**) is responsible for overseeing the implementation of this policy across the Trust, monitoring our compliance with data protection law, and developing related policies and guidelines for the Trust where applicable.

The DPO will provide an annual report of their activities directly to the Trust and, where relevant, report to the governing boards their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The Trust's DPO is Ian Turner, Director of People, Employee Engagement and PSTE and is contactable via ian.turner@rmt.org and [GDPR@rmt.org].

5.3 Senior Leaders

The Provision leads act as the representative of the data controllers on a day-to-day basis at the Trust's various sites, supported by the Executive Team, Council of Management and the Trust's GDPR Compliance Team.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties.
    -

6. Data protection principles

The GDPR is based on six data protection principles that the Trust must comply with. Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected and processed only for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date (any inaccurate data must be deleted or rectified without delay)
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Personal data of staff

We will collect and use the following types of personal data about the Trust's staff:

- recruitment information an application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- contact details and date of birth
- the contact details for emergency contacts
- gender
- marital status and family details
- information about contracts of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
- bank details and information in relation to tax status including national insurance number
- identification documents including passport and driving licence and information in relation to immigration status and right to work for the Trust
- information relating to disciplinary or grievance investigations and proceedings (whether or not a particular member of staff was the main subject of those proceedings)
- information relating to performance and behaviour at work
- training records
- electronic information in relation to use of IT systems/swipe cards/telephone systems
- images (whether captured on CCTV, by photograph or video); and
- any other category of personal data of which we may notify from time to time.

7.2 Special categories of personal data of staff

We may hold and use any of the special categories of personal data of staff in accordance with the law.

8. Collection and Processing of personal data

8.1 Lawfulness, fairness and transparency - how the Trust will process personal data

The Trust will process personal data (including special categories of personal data) in accordance with our obligations under the DPA 2018.

We will process personal data:

- for performing the contract of employment (or services) between us
- for complying with any legal obligation
- where it is necessary for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden – see details of individuals' rights in section 11 below).

We can process personal data for these purposes without an individual's knowledge or consent. We will not use such personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it.

We will only process special categories of personal data in certain situations in accordance with the law. For example, we can do so if we have explicit consent from an individual (or their parent/carer when appropriate in the case of a student/pupil). If the Trust has asked for consent to process a special category of personal data then we will provide all relevant information required by data protection law, including the reasons for our request. An individual does not need to consent and can withdraw consent later if they choose by contacting the DPO.

We do not need consent to process special categories of personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect an individual's vital interests or those of another person where they are physically or legally incapable of giving consent
- where an individual has made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of an individual's working capacity.

IF EMPLOYER INTENDS TO PROCESS INFORMATION ABOUT CRIMINAL CONVICTIONS THIS SHOULD BE EXPLAINED, ALONG WITH THE REASONS FOR IT.

We do not take automated decisions about you using personal data or use profiling.

8.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Data Retention Policy.

9. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil/student or parent/guardian/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils or for our legitimate interests. When doing this, we will require those companies to keep all personal data confidential and secure and to protect it in

accordance with the law and our policies. They are only permitted to process the data for the lawful purpose for which is has been shared and in accordance with our instructions.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. How should staff process personal data for the Trust?

Everyone who works for, or on behalf of, the Trust has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Trust's Data Security, Data Retention and Acceptable Use policies.

The Trust's DPO is responsible for reviewing this policy and updating the governing boards on the Trust's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be directed to the DPO.

All staff should take particular note of the following:

- Personal data covered by this policy should only be accessed if required for the work done by staff for, or on behalf of the Trust and only if that individual has been authorised to do so. The data should only be used for the specified lawful purpose for which it was obtained.
- Personal data should not be shared informally.
- Personal data must be kept secure and not be shared with unauthorised people.
- Every staff member should regularly review and update personal data which they have to deal with for work. This includes telling us if their own contact details change.
- Unnecessary copies of personal data should not be made. If copies are made, these should be kept and disposed of securely.
- All staff should use strong passwords.
- All computer screens should be locked when a staff member is not at their desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Personal data must never be saved to a staff member's own personal computer or other devices.

- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the DPO.
- All drawers and filing cabinets should be locked. Paper with personal data should not be left lying about.
- Personal data should not be taken away from Trust's premises without authorisation from your line manager or the DPO.
- Personal data should be shredded and disposed of securely when finished with.

Staff should ask for help from the DPO if they are unsure about data protection or if they notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

11. Subject access requests and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

The Trust must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a subject access request. However, if a request is manifestly unfounded or excessive the Trust may charge a reasonable administrative fee or refuse to respond to the request. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents/guardians or carers. For a parent/guardian or carer to make a subject access request with respect to a child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents/guardians or carers of pupils at any of the Trust's schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Subject access requests from parents/guardians or carers of children aged 12 and above may not be granted without the express permission of the pupil/student. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

11.3 Other data protection rights of the individual

An individual has the following rights:-

- To information about what personal data we process, how and on what basis as set out in this policy
- To access one's own personal data by way of a subject access request (see above)
- To correct any inaccuracies
- To request that we erase an individual's own personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected
- While requesting that an individual's personal data is corrected or erased or contesting the lawfulness of our processing, that individual may apply for its use to be restricted while the application is made
- To object to data processing where we are relying on a legitimate interest to do so and that individual considers their own rights and interests outweigh our own and wish us to stop
- To object if we process an individual's personal data for the purposes of direct marketing
- To receive a copy of an individual's own personal data and to transfer it to another data controller. We will not charge for this and will in most cases aim to do this within one month
- With some exceptions, not to be subjected to automated decision-making
- To be notified of a data security breach concerning an individual's own personal data
- In most situations we will not rely on an individual's consent as a lawful ground to process their data. If we do however request consent to the processing of an individual's personal data for a specific purpose, that individual has the right not to consent or to withdraw their consent later

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Everyone has the right to complain to the Information Commissioner. This can be done by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on individuals' rights and our obligations.

12. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012. Parents/guardians/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/guardians/carers and pupils can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any

relevant data already captured is deleted. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

13. CCTV

We use CCTV in various locations around the Trust's sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

14. Photographs and videos

As part of our Trust activities, we may take photographs and record images of individuals within our provisions.

For children
We will obtain written consent from parents/guardians/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

For adults
We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school/college on notice boards and in magazines, brochures, newsletters, etc.
- Outside of school/college by external agencies such as the photographer, newspapers, campaigns
- Online on our websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child/student, to ensure they cannot be identified.

See our Image Use Policy for more information on our use of photographs and videos.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Designating a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

Any member of staff who is aware of a data breach must contact the DPO immediately and keep any evidence they have in relation to the breach.

19. Training

All staff and members of the Trust's governing boards are provided with data protection training as part of their induction process.

Data protection also forms part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the DPA 2018). Otherwise, or from then on, this policy will be reviewed every 2 years and shared with all of the Trust's full governing boards.

21. Links with other policies

This data protection policy is linked to our:

- Data Security Policy
- Data Retention Policy
- Acceptable Use Policy
- Image Use Policy