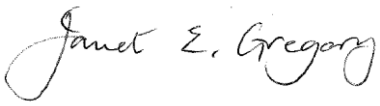
DATA PROTECTION POLICY
FREEDOM OF INFORMATION PUBLICATION SCHEME

Policy approved by the Chair of the Board May 2018
and will be ratified by the Board at the Trust meeting
on 19 July 2018
Signed



Janet Gregory
Chair of Trust Board

NEXT REVIEW – AUTUMN 2021

CRANMER EDUCATION TRUST

THE BLUE COAT SCHOOL, EGERTON STREET, OLDHAM. OL1 3SQ

Introduction

This policy is set into four separate sections:

Part 1 – Data Protection

Part 2 – Freedom of Information

Part 3 – Publication Scheme

Part 4 – Data Protection Officer

Part 1 Data Protection

1.1 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.
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.

1.2 Introduction

The Cranmer Education Trust is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) 2018. The Trust needs to process certain personal data about staff and pupils in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government. The Trust will process such information according to the Data Protection Principles that are set out in the GDPR.

When statements refer to the Trust they must be read to incorporate the member schools. The schools within the Trust are:

- The Blue Coat C of E School
- East Crompton St George C of E Primary School
- Mayfield Primary School

The Trust has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Trusts also have a duty to issue Privacy Notices to all pupils/ parents/staff, this summarises the information held on individuals, explains why it is held and the other parties to whom it may be passed on.

1.3 What is Personal Data?

Personal data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data

includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

1.4 Data Protection Principles

Article 5 of The General Data Protection Regulation 2018 Requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

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

It also requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

1.4 General Statement

The Trust is committed to maintaining the above principles always. Therefore, the Trust will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure staff are aware of and understand the relevant policies and procedures

1.5 Collecting personal data

1.5.1 Lawfulness, fairness and transparency

The Trust will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a **legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can **perform a task** in the public interest, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/guardian when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

1.5.2 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 to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

1.6 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 or parent/guardian 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 – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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
- Relating to 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 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.

1.7 Rights of access to information

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

1.7.1 Subject access request

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned

- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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 will not make a charge for the provision of information.

1.7.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to their 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 or guardians of pupils in these circumstances 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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, a majority subject access requests from parents or guardians of pupils at our Trust may not 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.

The Headteacher or nominee of the relevant school will discuss the request with the child and take their views into account when deciding on their capacity to understand. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

1.7.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification – see below 1.7.4

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month (not working or school days but calendar days, irrespective of school holiday periods) of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.
A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

1.7.4 Identification

The identity of the requestor must be established before the disclosure of any information, and checks will also be carried out regarding proof of relationship if the subject is a child. Evidence of identity will be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

(This list is not exhaustive)

1.7.5 Form of the information provided

- GDPR allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

- Third party information is that which has been provided by another, such as the police, local authority, health care professional or another school. Before disclosing third party information consent will normally be obtained. There is still a need to adhere to the 1-month statutory timescale.
- Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed, nor will information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
- If there are concerns over the disclosure of information, then additional advice will be sought.
- Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained to establish, if a complaint is made, what was redacted and why.
- Information disclosed will be clear, thus any codes or technical terms will be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it will be retyped.
- Information can be provided at the relevant school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
- The views of the applicant will be considered when deciding the method of delivery. If postal systems are required, then registered/ recorded mail must be used.

1.8 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 1.5), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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.

1.9. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012. Note that under this Act a "child" means a person under the age of 18.

Parents/guardians 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 guardian before we take any biometric data from their child and first process it.

Parents/guardians and pupils have the right to choose not to use the Trust's biometric systems. We will provide alternative means of accessing the relevant services for those pupils.

Parents/guardians and pupils can object to participation in the Trust's biometric recognition systems, 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)/guardian(s).

Where staff members or other adults use the Trust's biometric systems, 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.

1.10 CCTV

We use CCTV in various locations in the Trust 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 through each school's relevant CCTV policy. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

1.11 Photographs and videos

As part of our Trust activities, we may take photographs and record images of individuals within our Trust schools.
We will obtain written consent from parents/guardians, 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/guardian 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 on notice boards and in Trust/school magazines, brochures, newsletters, etc.

- Outside of the Trust by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust or relevant school's website 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, to ensure they cannot be identified.
The Trust has a Staff Mobile Devices and IT acceptable use policy for more information on our use of photographs and videos

1.12 Data protection by design and default

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

- Appointing 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 (see section 1.4)
- 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
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters
- 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 Trust and 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

1.13 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 classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the relevant school's office
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment see our Staff Mobile Devices and IT 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 (see section 1.6)

1.14 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.

1.15 Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.
When appropriate, we will report the data breach to the ICO within 72 hours.

1.16 Training

All staff, Trustees and Governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

Part 2 - Freedom of Information

The Freedom of Information Act 2000 (FoI) came fully into force on January 1 2005. Under the Act, any person has a legal right to ask for access to information held by the Trust. They are entitled to be told whether the Trust holds the information, and to receive a copy, subject to certain exemptions.

The information which the Trust routinely makes available to the public is included in the Publication Scheme (Part 3). Requests for other information will be dealt with in accordance with the statutory guidance. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information.

The Act is fully retrospective, so that any past records which schools hold are covered by the Act. The DfE has issued a Retention Schedule produced by the Records Management Society of Great Britain, to guide schools on how long they should keep school records.

It is an offence to wilfully conceal damage or destroy information to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed.

Requests must be made in writing, (including email), and should include the enquirers name and correspondence address, stating what information is required. They do not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether the information is held, and supplying any information that is held, except where exemptions apply. There is no need to collect data in specific response to a FoI enquiry. There is a time limit of 20 days excluding school holidays for responding to the request.

Obligations and Duties

The Trust, and its member schools, recognises its duty to:

- Provide advice and assistance to anyone requesting information. The Trust will respond to straightforward verbal requests for information, and will help enquirers to put more complex verbal requests into writing so that they can be handled under the Act.
- Tell enquirers whether it holds the information they are requesting (the duty to confirm or deny), and provide access to the information we hold in accordance with the procedures laid down.

Part 3 - Publication Scheme

The Trust has adopted the Model Publication Scheme for Schools approved by the Information Commissioner. The Publication Scheme and the materials it covers are detailed below.

This publication scheme commits the Trust to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the Trust.

The scheme commits the Trust:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the Trust and falls within the classifications below.

- To specify the information which is held by the Trust and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the Trust makes available under this scheme.
- To make this publication scheme available to the public.

Classes of information

- Who we are and what we do. Organisational information, locations and contacts, constitutional and legal governance.
- What we spend and how we spend it. Financial information relating to actual income and expenditure.
- What our priorities are and how we are doing. Strategy and performance information, plans, assessments, inspections and reviews.
- Our policies and procedures. Current written protocols for delivering our functions and responsibilities.
- Lists and registers. Information held in registers required by law and other lists and registers relating to the functions of the Trust.
- The services we offer. Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The Trust will indicate clearly to the public what information is covered by this scheme and how it can be obtained. Where it is within the capability of the Trust, information will be provided on our website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, we will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where the Trust is legally required to translate any information, it will do so. Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the Trust for routinely published material will be justified and transparent and kept to a minimum. Material which is published and accessed on a website will be provided free of charge. Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

How to request information

If you require a paper version of any information, or want to ask whether information is available, please contact the relevant school by telephone, email, fax or letter. Contact details are set out below.

The Blue Coat School

The Blue Coat School, Egerton Street, Oldham, OL1 3SQ
Email: secretary@blue-coat.org
Tel: 0161 624 1484

East Crompton St George C of E Primary School,

East Crompton St George C of E Primary School, George Street, Shaw, Oldham, OL2 8AX
Email: info@stgeorges.oldham.sch.uk
Tel: 01706 847 502

Mayfield Primary School

Mayfield Primary School, Mayfield Road, Oldham, OL1 4LG
Email: info@mayfield.oldham.sch.uk
Tel: 0161 624 6425

To help us process your request quickly, please clearly mark any correspondence "PUBLICATION SCHEME REQUEST"

Feedback and Complaints

The Trust welcomes any feedback or suggestions about the scheme. Any comments about the publication scheme, if further assistance is required, or to make a complaint, correspondence should be addressed to:

J A Hollis, CEO, Cranmer Education Trust, c/o The Blue Coat School, Egerton Street, Oldham, OL1 3SQ

Formal complaints may be made on the following grounds:

- Dissatisfaction with the assistance provided by the Trust
- The initial complaint has not been resolved

Formal complaints should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. They can be contacted at:

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Enquiry/ Information Line: 01625 545 700
E Mail: publications@ic-foi.demon.co.uk.
Website: www.informationcommissioner.gov.uk

Part 4 – Data Protection Officer (DPO)

The GDPR puts a duty on the Trust, as a public authority, to appoint a Data Protection Officer (DPO). The DPO assists the Trust to monitor internal compliance, inform and advise on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

The DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level of the trust.

The Trust has appointed Oldham Council's Information Management Service as the DPO. They are the key liaison point for the Information Commissioner's Office. They advise the trust on compliance with data protection legislation, individual rights, data security and breach handling policies.

Barbara Mulvihill
Data Protection Officer
Oldham Council
Civic centre
West Street
Oldham
OL1 1UG

Email: DPO@oldham.gov.uk

Tel: 0161 770 1311

Monitoring arrangements

The DPO will support the Trust in monitoring and reviewing this policy. This policy will be reviewed and updated if necessary if any changes are made to the law that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed every 3 years and approved by the Trust Board.