Salford Academy Trust

Data Protection Policy

And

Detailed Procedures

Data Protection Policy

Salford Academy Trust (the Trust) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the schools within the Trust.

The Trust is committed to the protection of all personal data for which it is responsible as the Data Controller in accordance with the General Data Protection Regulation (GDPR). The GDPR is an EU regulation that deals with the processing of personal information, which came into effect from 25 May 2018.

The schools in the Trust will only hold the minimum personal data necessary to enable them to perform the required educational functions and it will not hold data for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Scope

This policy applies to all the schools that form part of Salford Academy Trust; Irlam and Cadishead College, Albion Academy, Dukesgate Academy and Malborough Road Academy.

The policy applies to personal information regardless of the way it is collected, used, recorded, stored and destroyed, and it covers electronic, written and verbal records. It applies to all staff, volunteers and contractors who process information on behalf of the schools in the Trust.

Any failure to follow this policy may result in disciplinary proceedings, in accordance with our HR procedures.

What is personal information?

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

Data protection principles

The six data protection principles defined by the GDPR require that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; reasonable steps 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;
- 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; and
- 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.

This Data Protection policy and supporting procedures have been developed to outline how the Trust manages the personal information it processes in accordance with these principles.

Fair, lawful and transparent processing

All personal data the schools in the Trust use will be fairly obtained and lawfully processed in accordance with the conditions for processing outlined in the GDPR. We shall be transparent about the intended processing of data and will inform parents, pupils and our staff of the data we collect, process and hold, the purposes for which the data is held and the third parties (e.g. Local Authorities, the Department of Education) to whom it may be passed.

Our privacy notices will be communicated to parents, pupils and staff through our website and other appropriate communications. For example, pupil starter packs, letters, prospectus, data collection forms, HR communications to our staff, handbooks etc.

Processing, storing, and deleting personal information

All personal information stores within the Trust's control shall be identified as personal, special category (i.e. sensitive) or both. This will be recorded in the Trust's Personal Information Asset Register which is managed by our Data Protection Officer.

Personal data and records about pupils are confidential to the child and their parent or guardian. The information can be shared appropriately with people working for the Trust to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change school.

The Trust recognises that the secure disposal of redundant data is an integral element to compliance with the GDPR. All data held in any form of media (e.g. paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All personal data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Individual rights – e.g. subject access requests and other rights

Parent, pupils and staff have the right to request a copy of the personal data the Trust holds about them. This includes a description of that data, the purpose for which the data is processed, the sources of that data, to whom the data may be disclosed and a copy of all the personal data. We follow our Subject Access Request procedure when dealing with access requests.

Under certain circumstances under the GDPR parents, pupils and staff can also exercise rights in connection with the rectification, blocking, erasure, and destruction of personal data.

Data security

Information security around personal data is aligned to the Trust's Information Security and Acceptable Use Policies. ICT must be involved in review and approving the security measures around stores and any external transmissions of personal information.

When deciding appropriate security arrangements the Trust considers the type of the personal data stored and the risk of harm and distress to pupils, parents or staff if the confidentiality of the information were compromised. Access control restrictions are used on the Trust's systems and network drives holding personal data to limit access to those who need it for their job.

The Trust implements safeguards where personal information is transmitted electronically (e.g. encryption and password protection), including personal data transmitted to statutory bodies. Email attachments containing personal data must not be sent externally without management approval.

Security measures will be actively monitored to ensure that arrangements for both electronic and hard copy written personal data stores remain up to date and adequate.

Third parties and data transfers

There may be circumstances where the Trust is required either by law or in the best interests of our pupils or staff to pass information onto external authorities; for example Local Authorities, Department of Education, Ofsted or the Department of Health. These authorities have their own policies relating to the protection of any data that they receive or collect.

The security arrangements of third parties that the Trust uses to help with processing personal data are considered in line with the requirements of the GDPR. There must always be a contract or data sharing agreement with third party suppliers that includes a binding commitment to process personal data in compliance with the GDPR, and include the right for the Trust to request evidence to support this assertion. The Trust's DPO reviews all contracts to make sure there are adequate arrangements around data protection.

The need to share data relating to individuals to organisations outside of the Trust is clearly defined within our fair processing notices and the basis for sharing given.

The steps to deal with a request to share personal information on our pupils and staff are explained in our Third Party Disclosure procedures. A record is retained by our Data Protection Officer of all Third Party Disclosures.

Data protection impact assessments

The Trust uses a risk-based approach to assess the impact on data subjects associated with data processing personal information. This involves:

1. Analysis of the Trust's processes and systems that process personal information;
2. Focusing on high risk areas (e.g. holding sensitive personal data) which could cause damage or distress if not processed correctly;
3. Assessing any threats and vulnerabilities to the processing of personal data in these high risk areas;
4. Designing controls to mitigate risk and reduce the likelihood of non-compliance; and,
5. Ongoing monitoring of the effectiveness of these controls.

Data protection impact assessments are undertaken for significant changes in processes and systems at the Trust to ensure that data protection requirements are given consideration, in accordance with the GDPR principle "Data protection by design".

Breaches of personal information

The Trust's process for managing incidents involving personal information is made up of four key elements:

1. Containment of the initial incident;
2. Recovery from the incident;
3. An assessment of how the incident occurred, the ongoing risk and any reporting; and,
4. An evaluation of the effectiveness of the response.

The steps undertaken to manage and report on any incidents involving personal data are detailed in the Trust's Personal Data Breach Procedure. A record is retained by our Data Protection Officer of all data protection incidents and the associated response taken.

Individual responsibilities

Our Data Protection Officer has overall responsivity for making sure the standards outlined in this policy and our detailed procedures are applied and enforced throughout the Trust. Any incidents where these standards are not applied are reported to [TBC].

All staff are responsible for making sure they have read and understood this policy and our detailed procedures around handling personal information.

Training and awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings, briefings, inset days etc.
- Day to day support and guidance from the DPO to emphasise the importance of embedding data protection into the culture at the Trust

A record of the training for each member of staff is maintained by our DPO.

Complaints

Complaints to do with handling of personal information are dealt with in accordance with the Trust's complaints policy. Complaints relating to information handling may be referred to the Information Commissioners Office (the Supervisory Authority in the UK).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer and approved by the Head teacher, or nominated representative.

Contact

If you have any enquires in relation to this policy, please contact our Data Protection Officer [insert details] who will also act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk.

Definition of key data protection terms

Term	Meaning
Controller	The entity that determines the purposes, conditions and means of the processing of personal information. This is [insert school name]
Processor	Any entities that processes personal information on behalf of the school
Data Protection Officer	The person in the school who ensures that we are adhering to the policies and procedures out in the GDPR. For all academies this is David Rathbone based at Albion Academy.
Data subject	An identifiable natural person whose personal information is processed by the controller or processor. This includes pupils, parents, guardians, staff, governors, volunteers etc.
Personal data	Any information related to a Data Subject that can be used to directly or indirectly identify the person (see examples in Appendix D)
Special Category (Sensitive) personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, medical records and sex life or sexual orientation.
Subject Access Request	Entitles any data subject to have access to and information about the personal data that the school holds has concerning them

Data Protection Officer

Role and responsibilities

The main duties of our Data Protection Officer are:

- Co-ordinating the implementation, management and review of the Trusts' Data Protection Policy and detailed procedures.
- Making sure the Trust is lawful, fair and transparent in all its activities which involve handling personal information, and applies the six principles outlined in the General Data Protection Regulation.
- Providing data protection advice and assistance to colleagues across the Trust including:
    - School staff around handling personal data on pupils and their parents;
    - Human Resources on data protection aspects of procedures and employee documentation;
    - Projects that are implementing new processes and IT systems which involve processing personal data; and,
    - School sites when developing detailed procedures around g personal data and general data protection queries.
- Managing the Trust's Personal Data Asset Register, co-ordinating reviews and updates for new personal data collections.
- Communications from the Trust with the Information Commissioner.
- Co-ordinating delivery of data protection training and ongoing awareness to staff.
- Managing the response to subject access requests at any of the school sites or the Trust's offices.
- Managing the investigation and response to any data protection breaches at any of the school sites or the Trust's offices.
- Reviewing data protection clauses included in contracts and data sharing agreements.
- Managing complaints from parents, pupils or staff regarding the processing of their own (or their child's) personal data.
- Liaising with ICT and Internal Audit on data protection related matters.
- Assessing the adequacy of controls around personal data processing in due diligence reviews of potential third party providers.
- Performing or co-ordinating data protection risk assessment on processes identified as high risk and co-ordinating the resulting actions to address any weaknesses identified.

Subject Access Request Procedure

Background

The Trust is committed to the protection of all personal data for which it is responsible as the Data Controller in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

There are two distinct rights of access to information held by schools:

- Under Article 15 of the GDPR any individual has the right to make an access request to access the personal information held about them; and,
- The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

This procedure relate to subject access requests (SARs) made under the GDPR.

Separately from the GDPR, The Education (Pupil Information) (England) Regulation 2005 provides a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply in writing. For educational records (unlike other personal data) access must be provided within 15 Academy days, and if copies are requested, these must be supplied within 15 days of payment.

Scope

This procedure applies to the schools that form part of Salford Academy Trust; Irlam and Cadishead College, Albion Academy, Dukesgate Academy and Malborough Road Academy.

Responsibilities

It is the responsibility of our Data Protection Officer (DPO) to make sure these procedures are followed at all times. This is done through staff training and compliance monitoring. All staff must make sure that they have read, understood, and follow the procedures described in this document.

Handling a Subject Access Request

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility.

Before responding to a request for information held about a child from a parent or guardian, you should consider the child's capacity to understand and the nature of the request. This will vary from one child to another, but, as a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 12.

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. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

Where considered appropriate our Head teacher will discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. If you are confident that the child can understand their rights, then you should respond to the child rather than the parent.

A child can request access to his/her own personal data. Our DPO will judge whether the request is in the child's best interests, if the child will understand the information provided and consider whether the request has been made under coercion.

A member of the school's staff (or former member of staff) can request access to their own records at no charge, but the request must still be made in writing.

Receiving a request

All requests for personal information made to the school must be in writing, which can be by letter, email (or fax), and addressed to the DPO or Head teacher. You must never accept a verbal request. If this is queried explain that SARs must always be made in writing. A person's own written request is acceptable provided it gives us all the information needed, including proof of identify.

Where possible, tell the person to complete the school's SAR form and send it to our DPO at the address on the form. Explain that if they complete our form then this will allow us to respond to their request quicker. If the form is not used the school may need to contact them again to get the information we need. If this is queried you should advise that the 30 calendar day response deadline only starts when we have had the details that we need to help find all the information.

Validating and acknowledging the request

Where SARs concern access to a child's personal records the identity of the requestor must be established before the disclosure of any information Checks must also be carried out regarding proof of relationship to the child.

Evidence of identity must be evidenced by seeing a photo id such as:

- passport
- driving license

Plus evidence of their address:

- Bank statement, utility bill, council tax bill, credit card or mortgage statement, dated in last 3 months with their current address

And their relationship to child:

- Birth certificate

Checks should be made if a request for information is made by a parent, that there is no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.

Proof of identity (photo id and address) is also required for former members of staff making a SAR. Once identify has been verified there is no need to retain the documents used and they should be disposed of securely.

Once the required information to process the request has been received, it must be acknowledged in writing by sending out a standard letter to the applicant. If we do not have all the information needed to process the request a letter requesting additional information, along with the original application, must be sent back to the applicant.

Processing the request

The GDPR requires that all requests for personal information are dealt with within 30 days of receipt except requests for educational records (see above).

From 1st January 2005, when the Freedom of Information Act came into force, a request for personal information can include unstructured as well as structured records. This includes letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them.

Our DPO is responsible for working with staff and our third party processors to collate the information needed to respond to the request. This search must include information on our computer systems and databases, paper files, all information held in our archives and emails where the individual is the subject of the email.

The information must be printed out in hard copy and any abbreviations, codes or technical terms in the information that the individual may not understand must be annotated with a brief description. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

No information must be changed as the school must provide an accurate record of the information at the time of the request.

Reviewing before release

The information must be checked by the DPO before it is released. The names and any other details that would allow the applicant to identify any other individuals must be made unreadable (redacted)

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings

Certain information may be withheld under an exemption. For example, providing the information could prejudice prevention of detection of a crime, the information that is part of current negotiations with the requestor (e.g. redundancy, fees payable), or the information relates to legal advice concerning the person involved.

If there are concerns over the disclosure of information then additional legal advice should be sought.

Releasing the information

A photocopy of the information must be made for sending to requestor. A covering letter must be sent out with the information which provides an outline of the type's personal information we hold, what the information it is used for, and describe any organisations the information has been passed onto.

The information and the covering letter must be sent out to the address detailed on the SAR form by business secure post with proof of delivery. Even if our search identifies that we do not hold any personal information about the applicant we still need to send the applicant a letter explaining this.

Record keeping and reporting

The school documents all requests for personal information in a Subject Access Request Log as soon as they are received. This includes details of the requestor, date request received, the child (if applicable), who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.).

The original copy of the information collected should be kept in a permanent paper file along with the SAR form, in case of challenge from the applicant. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish what was redacted and why.

Keeping these records helps the school to deal with a complaint if one is made in relation to the request.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Contact

If you have any queries or concerns regarding these policies / procedures then please contact our Data Protection Officer.

Salford Academy Trust

Parents / Pupils
Subject Access Request Form

The General Data Protection Regulation provides individuals with rights over how their personal data is processed. These rights entitle you to a description of your personal data which we hold; the purposes for which it is used; and to whom your data may be disclosed. You are also entitled to obtain a copy the personal data we hold on you.

If you are a parent you may be able to request personal information we hold on your child under the GDPR. Before responding to a request for information held about a child from a parent or guardian, we may consider the child's capacity to understand and the nature of the request. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

To enable us to respond efficiently to your request, please:

1 Complete all the relevant sections of this form
2 Enclose a copy of the identification documents requested
3 Send the completed form and copies of required identification documents to:-

Subject Access Request
Data Protection Officer
Salford Academy Trust
Frontier House
Merchants Quay
Salford
M50 3SR

Section 1 – Data Subject Details	
Your Full Name:	
Address: Post Code:	
Tel:	Mobile:
Email:	
Childs full name (if applicable):	
School your child attends:	
Are you (delete as applicable): A current or former parent of a pupil? Yes/No A current or former staff member? Yes/No Another individual (please provide details):	

Proof of identity
Please provide copies of the following documents that verifies your name and address, and relationship to the pupil whose data is being requested (if applicable). Passport / driving licence photo page Utility Bill, Council Tax Bill, Credit Card Statement, Bank Statement (dated in last 3 months) Proof of relationship to child (if applicable (e.g. Birth Certificate)

Section 2 : Personal Data you are requesting
Please use this section to tell us what personal data you would like to see. "Personal Data" means information relating to the Data Subject as an individual. Please be a specific as possible as this will help speed up our response, include any notes to help us locate the information you are requesting, for example by listing the specific documents or information that you would like disclosed or the date period you are interested in.
Details of information requested (with dates)

Section 3 – Declaration	
I confirm that I am the Data Subject/ Parent/legal guardian of the pupil (delete as applicable) and that the information given on this form is correct and supplied the proof of identity requested.	
Signed:	Date:

Checklist – Please ensure that you have provided us with the following:

Description of the data you require	Yes/No
Dates relating to the data you require	Yes/No
Proof of identity and relationship to child	Yes/No
Signed declaration	Yes/No

Please note:
Salford Academy Trust reserves the right to obscure or suppress information that relates to third parties. Personal information collected on this form is required to enable your Subject Access Request to be processed, and will only be used in conneciton with this request.

Salford Academy Trust's Data Protection Policy is available on our website Salford Academy Trust or on request if you contact us. In accordance with the GDPR, we may take up to 30 days to respond to your request. Requests will only be considered live when we have received sufficient information to verify your identity and the information you are seeking.

Office use only:

Request received:
Date completed:
Notes:

Salford Academy Trust

Current / Former Member of Staff
Subject Access Request Form

The General Data Protection Regulation provides individuals with rights over how their personal data is processed. These rights entitle you to a description of your personal data which we hold; the purposes for which it is used; and to whom your data may be disclosed. You are also entitled to obtain a copy the personal data we hold on you.

To enable us to respond efficiently to your request, please:

1 Complete all the relevant sections of this form
2 Enclose a copy of the identification documents requested
3 Send the completed form and copies of required identification documents to:-

Subject Access Request
Data Protection Officer
Salford Academy Trust
Frontier House
Merchants Quay
Salford
M50 3SR

Section 1 – Data Subject Details	
Your Full Name:	
Address: Post Code:	
Tel:	Mobile:
Email:	
School you work / worked at:	
Are you (delete as applicable): A current member of staff? Yes/No A former member of staff? Yes/No Another individual (please provide details):	
Proof of identity	
Please provide copies of the following documents that verifies your name and address: Passport / driving licence photo page Utility Bill, Council Tax Bill, Credit Card Statement, Bank Statement (dated in last 3 months)	

Section 2 : Personal Data you are requesting
Please use this section to tell us what personal data you would like to see. “Personal Data” means information relating to the Data Subject as an individual. Please be a specific as possible as this will help speed up our response, include any notes to help us locate the information you are requesting, for example by listing the specific documents or information that you would like disclosed or the date period you are interested in.
Details of information requested (with dates)

Section 3 – Declaration	
I confirm that I am the Data Subject/ Parent/legal guardian of the pupil (delete as applicable) and that the information given on this form is correct and supplied the proof of identity requested.	
Signed:	Date:

Checklist – Please ensure that you have provided us with the following:

Description of the data you require	Yes/No
Dates relating to the data you require	Yes/No
Signed declaration	Yes/No

Please note:
Salford Academy Trust reserves the right to obscure or suppress information that relates to third parties. Personal information collected on this form is required to enable your Subject Access Request to be processed, and will only be used in conneciton with this request.

Salford Academy Trust’s Data Protection Policy is available on our website Salford Academy Trust or on request if you contact us. In accordance with the GDPR, we may take up to 30 days to respond to your request. Requests will only be considered live when we have received sufficient information to verify your identity and the information you are seeking.

Office use only:

Request received:
Date completed:
Notes:

Third Party Disclosure Procedure

Background

The Trust is committed to the protection of all personal data for which it is responsible as the Data Controller in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

This document outlines the procedures for responding to requests for personal information from statutory bodies and other third parties. This document defines:

- The roles and responsibilities when handling requests for personal information that are not from a parent/guardian, pupil or member of staff;
- Circumstances where exemptions apply to disclosing personal information under the GDPR and UK legislation; and
- The procedures to be followed when dealing with a request to disclose personal information.

The need to share data relating to individuals to organisations outside of our school shall be clearly defined within our fair processing notices and details of the basis for sharing given.

Scope

This procedure applies to the schools that form part of Salford Academy Trust - Irlam and Cadishead College , Albion Academy, Dukesgate Academy and Malborough Road Academy.

Responsibilities

It is the responsibility of our Data Protection Officer (DPO) to make sure these procedures are followed at all times. This is done through staff training and compliance monitoring. All staff must make sure that they have read, understood, and follow the procedures described in this document.

Procedures for disclosure of personal information

Personal data about pupils will not be disclosed to third parties without the explicit consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Pupil's personal data may be disclosed to the following third parties when there is a legal basis:

Department of Education - Schools is required to pass data to the Department of Education the Education and Skills Funding Agency (an executive agency of the DfE), and any successor bodies to these organisations, in order to help the government to monitor the national educational system and enforce laws relating to education.

Examination authorities - This is needed for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Local authorities, social workers, and support agencies - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data about pupils on to local authorities or support agencies.

The trust may also share personal data if a pupil transfers to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Personal data must not be disclosed to unauthorised third parties, including family members, friends and external organisations without documented consent from the pupil or their parent.

A record is kept of all approved personal information disclosures to keep track of what can be legitimately shared. The Third Party Disclosure log must be maintained of all disclosures of personal information to statutory bodies and any other third parties.

Receiving a request

Statutory bodies and other third parties requesting personal information from the school must always provide evidence of their identity and legal right to access the data. The request must be in writing (e.g. letter, email) and include:

- Name and Address of the organisation;
- Telephone number;
- Details or the person requesting the information (name, job title, proof of identity);
- Legal powers supporting the disclosure request; and,
- A declaration of liability that, once shared, they responsible for the processing of the information in accordance with the GDPR and any other relevant legislation).

If you are ever unsure over the identity of the requestor telephone the organisation making the request to validate they are who they say they are. Personal information must never be given out to a third party over the telephone. Where a request is received over the telephone you must explain that it is the school's policy not to respond to telephone enquiries, and explain that a written request needs to be submitted.

Requests from the Police

Personal information requests from the Police to assist with their investigations must be passed on to be dealt with by the DPO. The DPO can then decide how to respond to the request.

Where a telephone request is received in an emergency from the Police, you must explain that you need proof to confirm the identity of the caller. This should be done by asking for their name, rank and identification number, and a switchboard number that they can be called back on with the information once it has been collected.

An emergency is defined as a situation that could cause harm or distress to the individual or a relative of the individual concerned.

Request from public sector bodies

Public sector bodies including Local Authorities, the DfE (and associated agencies), the Child Support Agency, and Health Authorities have the right to demand personal information from the school under a data protection exemption.

The body requesting personal information must make the request in writing and outline the statutory powers that apply to their request.

Request from HMRC

HMRC have the power to demand personal information to help carry out its statutory duties under the Taxes Management Act 1970. All requests from the HMRC relating to members of staff (current

and former) must be referred onto the Payroll team. The Third Party Disclosure log must be maintained of all disclosures of personal information to the HMRC.

Dealing with court orders

Where a court order is presented by the Police or another party this must be complied with as it is a legal demand for information. Court orders must be passed to the DPO.

Requests from other third parties

Any requests from solicitors or other third parties for personal information must be referred to the DPO to establish whether school is obliged to respond.

Data sharing with new third parties

A risk assessment must be performed in advance of sharing personal information with any new third parties, to understand the adequacy of their controls around data processing. There must always be a contract or data sharing agreeing that includes a binding commitment to process personal data in compliance with the GDPR. The Trust's DPO reviews all contracts to make sure there are adequate arrangements around data protection.

Record keeping

The Third Party Disclosure log must be completed whenever personal information is passed onto a third party. This includes:

- The date the disclosure request was received;
- The organisation and individual who received the information;
- What personal information was handed over;
- Who made the disclosure;
- The date the information was handed over;
- The justification that supports the disclosure; and,
- Any paperwork supporting the justification must be securely stored with the original request form.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Contact

If you have any queries or concerns regarding these policies / procedures then please contact our Data Protection Officer.