The Liverpool Joint Catholic and Church of England Academies Trust

Diocese of Liverpool

Data Protection Policy

Review Period:	**Two Yearly**
Person Responsible For Policy:	**Trust Director of Finance and Resources**
Governing Committee:	**Trust Board**
Date of Trustees Approval:	**March 2017**
Date for Review:	**March 2019**

Statement of intent

The Liverpool Joint Catholic and Church of England Academies Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998.

This policy will outline how The Liverpool Joint Catholic and Church of England Academies Trust will comply with the key principles of the Data Protection Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to the data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Data controller

The Trust as the corporate body is the Data Controller. The Board of The Liverpool Joint Catholic and Church of England Academies Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Trust Director of Finance and Resources will deal with the day-to-day matters relating to data protection.

Definitions

- *Personal data* is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

- *Sensitive personal data* is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

Staff responsibilities

The Liverpool Joint Catholic and Church of England Academies Trust recognises that its staff members and pupils need to know what The Trust does with the information it holds about them.

Staff members and parents are responsible for checking that any information that they provide to The Trust in connection with their employment or in regard to a registered pupil is accurate and up-to-date.

The Trust cannot be held accountable for any errors unless the employee or parent has informed The Trust about such changes.

Fair Processing

The Trust is committed to being clear and transparent about what type of personal information we hold and how it is used. The following 'Privacy Notice for Pupils and their Parents and Guardians' will be published on the Trust Website as part of this policy.

Privacy Notice for Pupils and their Parents and Guardians

Why do we collect information?

The Trust collects information about our pupils and holds this personal data so that we can:

- Support each pupil's learning;
- Monitor and report on each pupil's progress;
- Provide appropriate pastoral care and other support to each of our pupils; and
- Assess how well each pupil is doing and report on that to the parents.

What type of information do we collect?

The information will include: personal data such as name and date of birth as well as contact details; educational performance assessments; attendance information; pastoral information. It will also include sensitive personal data such as: ethnicity; special educational needs; behavioural incidents; and medical information that will help us to support each pupil's education and wider welfare needs at the Trust.

We will also hold personal contact information about parents and carers so that we can get hold of you routinely or in an emergency.

Where CCTV is used by the Trust this will only be for general security purposes in order to protect the pupils and staff of the Trust.

Pupil photographs may be included, as part of their personal data and this will be treated with the same level of confidentiality as all other personal data. Photographic images of pupils used in publically available media such as web sites, newsletters or the school prospectus will not identify pupils unless parental permission has been given in advance.

Do we share this information with anyone else?

We do not share any of this data with any other organisation without your permission except where the law requires it. We are required to provide pupil data to central government through the Department for Education (DfE www.education.gov.uk) and the Education Funding Agency (EFA www.education.gov.uk/efa). Where it is necessary to protect a child, the Trust will also share data with the Local Authority Children's Social Services and/or the Police.

Can we see the personal data that you hold about our child?

All pupils have a right to have a copy of the personal information held about them. As our pupils are of secondary school age, a request for a copy of the personal information has to be made by a parent or guardian in writing. The only circumstances under which the information would be withheld would be if there was a child protection risk, specifically:

- The information might cause serious harm to the physical or mental health of the pupil or another individual;
- Where disclosure would reveal a child is at risk of abuse;
- Information contained in adoption or parental order records;
- Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and
- Copies of examination scripts.

If you want a printed copy of the personal data then the Trust will charge the actual cost of providing the copy up to a maximum of a £10 charge. To protect each child's right of confidentiality under law the Trust reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed and any fee due paid, the information will be collected and provided within 40 calendar days.

Can we see our child's educational record?

All parents are also entitled to a copy of their child's educational record. A request must be made in writing to the Trust Board. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the Trust. Only information that has come from a teacher or employee of the Trust or an educational professional contracted by the Trust can be considered to form part of the educational record.

The Trust will charge a fee to provide an actual copy of the educational record but this will not be greater than the actual cost of reproducing the information. Once any fee has been received the Trust will respond to the request within 15 school days (21 calendar days excluding any public or Trust holidays).

Information Security

Objective

The information security objective is to ensure that the Trust's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Responsibilities

The Trust Director of Finance and Resources, in collaboration with the Executive Headteacher of the Trust has direct responsibility for maintaining the Information Security policy and for ensuring that staff within the Trust adheres to it.

General Security

It is important that unauthorised people are not permitted access to Trust information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

- Not reveal building entry codes to people that you do not know or who cannot prove themselves to be employees;
- Beware of people tailgating you into the building or through a security door;
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
- Not position screens on reception desks where members of the public could see them;
- Lock secure areas when you are not in the office;
- Not let anyone remove equipment or records unless you are certain who they are;

Visitors and contractors in Trust buildings should always sign in a visitor's book.

Security of Paper Records

Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;

Always keep track of files and who has them;

Do not leave files out where others may find them;

Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Security of Electronic Data

Most of our data and information is collected, processed, stored, analyzed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. Trust staff must:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;
- Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;

When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.

Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:

- Don't write it down;
- Don't give anyone your password;
- Your password should be at least 8 characters;
- The essential rule is that your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;
- You can be held responsible for any malicious acts by anyone to whom you have given your password;
- Include numbers as well as letters in the password;
- Take care that no-one can see you type in your password;
- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.
- Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

Use of E-Mail and Internet

The use of the Trust's e-mail system and wider Internet use is for the professional work of the Trust. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the Trust's wider policies are a requirement whenever the e-mail or Internet system is being used. The Trust uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling

content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately. The Trust Head of ICT will ensure that the sites are reported to the broadband provider for filtering.

To avoid a computer virus arriving over the Internet:

- Do not open any flashing boxes or visit personal websites;
- Do not send highly confidential or sensitive personal information via e-mail;
- Save important e-mails straight away;
- Unimportant e-mails should be deleted straight away;
- Do not send information by e-mail which breaches the Data Protection Act. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

Electronic Hardware

All hardware held within Trust should be included on the asset register. When an item is replaced, the register should be updated with the new equipment removed or replaced. Do not let anyone remove equipment unless you are sure that they are authorized to do so. In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desktops.

Homeworking Guidance

If staff must work outside of the Trust or at home, all of the 'Information Security' policy principles still apply. However, working outside of the Trust presents increased risks for securing information. The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
- Remote log-in should be used so confidential documents do not have to be taken off side whenever possible so data is still being held securely on the Trust servers.
- If you use a laptop or tablet or smart phone:
    - Ensure that it is locked and password protected to prevent unauthorised access;
    - Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the Trust;
    - Portable devices or memory sticks that contain personal data must be encrypted. Personal data may not be taking off the Trust's site or put onto a portable device without the express permission of the Trust Director of Finance and Resources. Taking personal data off-site on a device or media that is not encrypted may be a disciplinary matter.
    - Ensure personal data is not stored on the hard drive;
- When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.

Audit of Data Access

Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

Data Backup

The Trust will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the Trust is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

Data backup should routinely be managed on a rolling daily process to secure off-site areas.

Disposal of Information

Paper records should be disposed of with care. If papers contain confidential or sensitive information they must be placed in the confidential bins for secure collection or shredded before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

Where a third party contractor holds personal information on behalf of the Trust, for example a payroll provider, the Trust will seek reassurance from the contractor regarding their data protection policies and procedures.

Subject Access Requests

Requests from parents or pupils for access to personal data or educational records will be dealt with as described in the Privacy Notice for Pupils and their Parents and Guardians.

Trust staff may have access to their personal data within 40 calendar days of a request and at no charge.

The Trust will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

Sharing Personal Information

The Trust only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the Trust to carry out a function of the Trust.

The Trust is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.

Because our pupils are of secondary school age, their own right to access their own personal information held by the Trust will be exercised through their parents or guardians.

The Executive Headteacher, Trust Director of Finance and Resources or Heads of School will be responsible for authorising the sharing of data with another organisation. The principle, in authorising the sharing of data will take account of:

- Whether it is lawful to share it;
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;

Considerations regarding the method of transferring data should include:

- If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.
- Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

Websites

The Trust website will be used to provide important information for parents and pupils including this policy and Privacy Notice.

Where personal information, including images, are placed on the web site the following principles will apply:

- We will not disclose personal information (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;
- Comply with regulations regarding cookies and consent for their use;
- Our website design specifications will take account of the principles of data protection.

CCTV

If the Trust uses CCTV this will be notified to the Information Commissioners Office along with the purpose of capturing images using CCTV. The Trust appreciates that images captured on CCTV constitute personal information under the Data Protection Act.

Photographs

The Trust may use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications without further specific consent being sought.

Images recorded by parents using their own personal equipment of their child in a school play or activity for their own family use are not covered by data protection law.

All other uses by the Trust of photographic images are subject to data protection.

Processing by Others

The Trust remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of the Trust will have to specify how they will ensure compliance with data protection law.